Avira AntiVir Server | Unix

Avira AntiVir Professional | Unix

Handbuch für Anwender



Inhaltsverzeichnis

1 Über dieses Handbuch

In diesem Kapitel erhalten Sie einen Überblick über Aufbau und Inhalt des Handbuchs.

Nach einer kurzen Einleitung erhalten Sie Informationen zu folgenden Themen:

- Aufbau des Handbuchs – Seite 3
- Zeichen und Symbole – Seite 4

1.1 Einleitung

In diesem Handbuch haben wir für Sie alle nötigen Informationen zu Avira AntiVir Server/ Professional zusammengestellt und führen Sie Schritt für Schritt durch Installation, Konfiguration und Bedienung der Software.

Im Anhang finden Sie ein Glossar, das Ihnen grundlegende Begriffe erläutert.

Weitere Informationen und Hilfestellung bieten Ihnen darüber hinaus unsere Webseite, die Hotline unseres Technischen Supports und unser regelmäßiger Newsletter (siehe Service – Seite 51).

Ihr Team von Avira

1.2 Aufbau des Handbuchs

Das Handbuch zu Ihrer AntiVir-Software besteht aus mehreren Kapiteln, in denen Sie folgende Informationen finden:

Kapitel	**Inhalt**
1 Über dieses Handbuch	Aufbau des Handbuchs, Zeichen und Symbole.
2 Produktinformationen	Allgemeine Hinweise zu Avira AntiVir Server/ Professional, seinen Modulen, Leistungsmerkmalen und Systemvoraussetzungen sowie zur Lizenzierung.
3 Installation	Anleitung zur Skript-basierten Installation von AntiVir Server auf Ihrem System.
4 Konfiguration	Hinweise zur optimalen Anpassung der AntiVir-Komponenten an Ihr System.
5 Bedienung	Befehle und Parameter zum Ausführen des Guards und Scanners; Vorgehen beim Erkennen von Viren und unerwünschten Programmen.
6 Aktualisierungen	Aktualisierung per Internet und Intranet.
7 Das Kernel-Modul Dazuko	Kompilieren und Bedienen von Dazuko.
7 Service	Support und Service von Avira GmbH
8 Anhang	Glossar mit Erläuterungen von Fachbegriffen und Abkürzungen, Goldene Regeln zum Schutz vor Viren.

1.3 Zeichen und Symbole

In diesem Handbuch werden folgende Zeichen und Symbole verwendet:

Symbol	Erläuterung
✓	... steht vor einer Voraussetzung, die vor dem Ausführen einer Handlung erfüllt sein muss
▶	... steht vor einem Handlungsschritt, den Sie ausführen
↳	... steht vor einem Ergebnis, das direkt aus der vorangehenden Handlung folgt
	... steht vor einer Warnung bei Gefahr von kritischem Datenverlust oder Schäden an der Hardware
!	... steht vor einem Hinweis mit besonders wichtigen Informationen, z. B. zu den folgenden Handlungsschritten
i	... steht vor einem Tipp, der das Verständnis und die Nutzung von AntiVir erleichtert.

Zur besseren Lesbarkeit und eindeutigen Kennzeichnung werden im Text außerdem folgende Hervorhebungen verwendet:

Hervorhebungen im Text	Erläuterung
Strg+Alt	Taste bzw. Tastenkombination
/usr/lib/AntiVir/avscan	Dateinamen und Pfadangaben
`ls /usr/lib/AntiVir`	Eingaben des Anwenders
http://www.avira.de	URLs
Signs and Symbols – Seite 4	Querverweise innerhalb des Dokuments

1.4 Abkürzungen

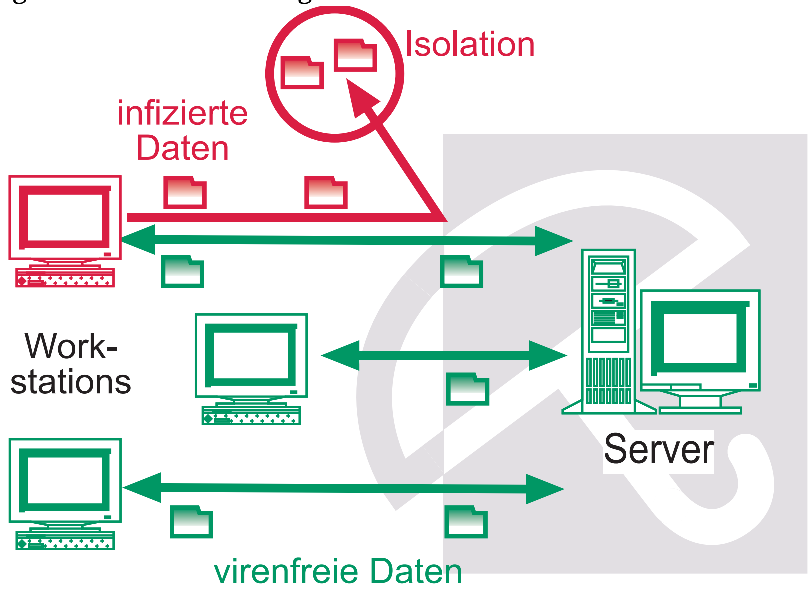
In diesem Handbuch werden folgende Abkürzungen verwendet:

Abkürzung	Erläuterung
CLS	Command Line Scanner (Kommandozeilen-Scanner)
FAQ	Frequently Asked Questions
GUI	Graphical User Interface
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
VDF	Virus Definition File

2 Produktinformationen

Sie sind zuständig für eine Vielzahl von Workstations und Servern im Netzwerk. Doch auch Sie haben nur zwei Augen. Die Server sind das Herz des Netzwerks. Können beispielsweise Viren hier ungehindert eindringen und sich verbreiten, ist es nur ein kleiner Schritt bis zum Infarkt des Netzwerks. Hiervor schützen die Produkte von AntiVir für Server.

Immer öfter nehmen UNIX-Rechner die Funktion z. B. von File-Servern oder Email-Gateway-Servern ein. Sie transportieren und lagern also auch Daten, die nicht im direkten Zusammenhang mit UNIX stehen, z. B. Dokumente aus Office-Paketen und Email-Attachments. Viren können dann auf einem Windows-Client, der auf den Server zugreift, ungehindert ihr Zerstörungswerk ausführen.



Avira AntiVir Server/ Professionalist ein umfassendes und flexibles Werkzeug, um der Gefahr von Viren und unerwünschten Programmen zu begegnen und Ihr System zuverlässig zu schützen.



Der Verlust wertvoller Daten hat meist dramatische Folgen. Auch das beste Virenschutzprogramm kann Sie nicht hundertprozentig vor Datenverlust schützen.

▶ Fertigen Sie grundsätzlich regelmäßig Sicherungskopien (Backups) Ihrer Daten an.



Ein Virenschutzprogramm ist nur dann zuverlässig und wirksam, wenn es aktuell ist.

▶ Stellen Sie die Aktualität von AntiVir über automatische Updates sicher. Sie erfahren in diesem Handbuch, was Sie hierfür tun müssen.

2.1 Leistungsumfang

Avira AntiVir Server/ Professional bietet umfangreiche Konfigurationsmöglichkeiten, damit Sie die Kontrolle über Ihr Netzwerk behalten.

Die wesentlichen Leistungsmerkmale von Avira AntiVir Server/ Professionall:

- Einfache Installation durch Installationsskript.
- Kommandozeilengestützter Scanner (On-Demand):
  Konfigurierbare Suche nach allen bekannten Typen sog. "Malware" (Viren, Trojaner, Backdoor-Programme, Hoaxe, Würmer usw.)
- Residenter Wächter (On-Access):
  Konfigurierbare Reaktionen auf den Fund von Viren und unerwünschten Programmen: Reparieren, Verschieben, Umbenennen von Programmen oder Dateien; automatisches Entfernen von Viren und unerwünschten Programmen.
- Heuristische Makroviren-Erkennung.
- Erkennt alle gebräuchlichen Archivtypen mit einstellbarer Rekursionstiefe bei verschachtelten Archiven.
- Einfache Integration in automatisierte Aufgaben (Jobs) wie definierte Suchläufe zu festgelegten Zeiten.
- Automatische Internet-Updates der Produkt-Komponenten, Engine und VDF-Dateien.
- Umfassende Protokoll-, Warn- und Benachrichtigungsfunktionen für den Administrator; Versenden von Warnungen per Email (SMTP)
- Schutz vor Änderungen der Programmdateien durch intensiven Selbsttest

2.2 Lizenzierungskonzept

Um AntiVir zu nutzen, benötigen Sie eine Lizenz. Sie erkennen damit die Lizenzbedingungen an
(siehe http://www.avira.com/documents/general/pdf/de/avira_eula_de.pdf).

Sie können die vielfältigen Funktionen von Avira AntiVir Server/ Professional mit folgenden Lizenz-Modellen nutzen:

- Testversion
- Vollversion

Die Lizenzierung ist abhängig von der Anzahl der Benutzer im Netzwerk, die durch AntiVir geschützt werden sollen.

Die Lizenz wird über die Lizenzdatei *hbedv.key* vergeben. Diese erhalten Sie von Avira GmbH per Email. Sie enthält genaue Angaben, welche Programme Sie für welchen Zeitraum lizenziert haben. Sie kann also auch die Lizenz für mehrere Produkte von Avira GmbH enthalten.

Testversion

30-Tage-Testlizenz für Avira AntiVir Server/ Professional.

Nähere Informationen zur Test-Lizenz erhalten Sie auf unserer Webseite http://www.avira.de.

Vollversion

Zum Leistungsumfang einer Vollversion gehören:

- Bereitstellung der AntiVir-Version zum Download aus dem Internet

- Lizenzdatei per Email zur Freischaltung von der Testversion auf die Vollversion
- Ausführliche Installationsanleitung (digital)
- Bereitstellung von PDF-Handbüchern zum Download aus dem Internet
- Vierwöchiger Installationssupport ab Kaufdatum
- Newsletter-Service (per Email)
- Update-Service auf die Programmdateien und die VDF per Internet

2.3 Module und Funktionsweise von Avira AntiVir Server/ Professional

Das Schutzpaket Avira AntiVir Server/ Professional besteht aus folgenden Programmteilen:

- AntiVir Engine
- AntiVir Guard
- AntiVir Kommandozeilenscanner
- Avira Updater

AntiVir Engine

Die AntiVir Engine umfasst im Wesentlichen die Prüf- und Reparaturmodule der Avira-Software. Diese Module werden auch von anderen AntiVir-Produkten verwendet.

AntiVir Guard

AntiVir Guard läuft im Hintergrund. Er prüft während des Zugriffs des Anwenders aus dem Netzwerk (on Access) permanent Dateien auf Viren und unerwünschte Programme. Der Zugriff auf betroffene Dateien wird sofort gesperrt. Die Dateien können automatisch umbenannt, repariert oder verschoben werden.

AntiVir Kommandozeilenscanner

Der Kommandozeilenscanner kann jederzeit aus der Kommandozeile aufgerufen werden (on Demand). Betroffene Dateien oder verdächtige Makros können über eine Vielzahl von Optionen gezielt isoliert, repariert oder gelöscht werden. Er kann in Skripte eingebunden und von Skripten ausgewertet werden.

Avira Updater

Der Avira Updater lädt in regelmäßigen Zeitabständen die neuesten Aktualisierungen von den Avira-Webservern herunter und installiert sie (manuell oder automatisch). Das Modul kann auch Benachrichtigungen per E-Mail versenden. Sie können Avira AntiVir insgesamt oder auch nur den Scanner aktualisieren.

2.4 Systemvoraussetzungen

Avira AntiVir Server stellt für einen erfolgreichen Einsatz folgende Mindestanforderungen an den Server:

- Rechner mit CPU ab i386 (Linux) oder Sparc (SunOS)
- 200 MB freier Speicherplatz auf der Festplatte
- 40 MB temporärer Speicherplatz auf der Festplatte
- 256 MB (512 MB unter SunOS) freier Hauptspeicher
- Linux mit glibc; SunOS

Die folgenden Distributionen sind für Avira AntiVir Server offiziell unterstützt:

- Red Hat Enterprise Linux 5 Server
- Red Hat Enterprise Linux 4 Server
- Novell SUSE Linux Enterprise Server 10 - 10.2
- Novell SUSE Linux Enterprise Server 9
- Debian GNU/Linux 4 (stabil), Debian etch
- Ubuntu Server Edition 8
- Sun Solaris 9 (SPARC)
- Sun Solaris 10 (SPARC)
- Novell Open Enterprise Server

Avira AntiVir Professional stellt für einen erfolgreichen Einsatz folgende Mindestanforderungen an den Server:

- Rechner mit CPU ab i386 (Linux) oder Sparc (SunOS)
- 100 MB freier Speicherplatz auf der Festplatte
- 20 MB temporärer Speicherplatz auf der Festplatte
- 192 MB (512 MB unter SunOS) freier Hauptspeicher
- Linux mit glibc; SunOS



Sie benötigen ausreichend Speicherplatz auf Ihrer Festplatte, um die temporären Dateien des Guards zu speichern. Wir empfehlen daher, mindestens 4 GB für das Verzeichnis temporärer Dateien einzuplanen.

Die folgenden Distributionen sind für Avira AntiVir Professionaloffiziell unterstützt:

- Red Hat Enterprise Linux 5 Desktop
- Red Hat Enterprise Linux 4 Desktop
- Novell SUSE Linux Enterprise Desktop 10 - 10.2
- Novell SUSE Linux Enterprise Desktop 9
- Debian GNU/Linux 4 (stable)
- Ubuntu Desktop Edition 8
- Sun Solaris 9 (SPARC)
- Sun Solaris 10 (SPARC)

2.5 Technische Informationen

Der AntiVir Guard basiert auf DazukoFS (http://www.dazuko.org), einem Open-Source-Softwareprojekt. DazukoFS ist ein Kernel-Modul, das die Dateizugriffe an den AntiVir-Guard-Dämon weiterleitet.

3 Installation

Die aktuelle Version von Avira AntiVir Server/ Professional ist im Internet verfügbar: www.avira.de.

AntiVir wird als gepacktes Archiv zur Verfügung gestellt. Dieses Archiv enthält die Engine, den Guard, den Kommandozeilenscanner und den Avira Updater.

Sie werden Schritt für Schritt durch die Installation geführt. Dieses Kapitel ist untergliedert in folgende Abschnitte:

- AntiVir erneut installieren oder deinstallieren – Seite 15
- Lizenzierung – Seite 9
- AntiVir installieren – Seite 10
- AntiVir erneut installieren oder deinstallieren – Seite 15
- Anbindung an AMaViS – Seite 16

3.1 Installationsdateien bereitstellen

Programmdatei aus dem Internet laden

Laden Sie die aktuelle Avira AntVir Server/Professional Version von unserer Webseite http://www.avira.com auf Ihren lokalen Rechner.
Speichern Sie die Datei in dem Verzeichnis für temporäre Dateien (*/tmp*) auf dem Computer, auf dem Sie AntiVir Server/ Professional installieren wollen. Zurzeit heißt diese Datei
antivir-server-prof-<version>.tar.gz
oder:
antivir-workstation-prof-<version>.tar.gz

Programmdatei entpacken

▶ Wechseln Sie in das temporäre Verzeichnis:
`cd /tmp`

▶ Entpacken Sie die Archivdatei für das AntiVir-Paket:
`tar -xzvf antivir-server-prof-<version>.tar.gz`
or:
`tar -xzvf antivir-workstation-prof-<version>.tar.gz`

↳ Ein Verzeichnis *antivir-server-prof-<version>* or *antivir-workstation-prof-<version>* wird im temporären Verzeichnis angelegt.

3.2 Lizenzierung

Sie müssen AntiVir lizenzieren, um es nutzen zu können (siehe Lizenzierungskonzept – Seite 6). Hierfür benötigen Sie eine Lizenzdatei *hbedv.key*.

Diese Lizenzdatei enthält Informationen zu Umfang und Dauer der Lizenz.

Lizenz erwerben

▶ Kontaktieren Sie uns telefonisch oder per Email (sales@avira.com), um eine gültige Lizenzdatei für Avira AntiVir Server/ Professional zu erhalten.

↳ Sie erhalten eine Lizenzdatei per Email zugesandt.

- Sie können Avira AntiVir Server/ Professional auch einfach und schnell über unseren Online-Shop erwerben (weitere Informationen siehe http://www.avira.de).

Lizenzdatei einspielen

- Kopieren Sie die Lizenzdatei *hbedv.key* in Ihr Installationsverzeichnis *./tmp/antivir-server-prof-<version>*
  or in *./tmp/antivir-workstation-prof-<version>*.



Sie können die Installation auch ohne Lizenzdatei durchführen. Die Lizenzdatei kann nachträglich in das AntiVir-Programmverzeichnis */usr/lib/AntiVir* kopiert werden.

3.3 AntiVir installieren

Die Installation von AntiVir läuft weitgehend automatisch über ein Installationsskript ab. Dieses Skript führt folgende Aufgaben durch:

- Prüfen der Installationsdateien auf Vollständigkeit.
- Prüfen, ob Sie ausreichende Rechte zur Installation besitzen.
- Prüfen, inwieweit schon eine Version von AntiVir auf dem Rechner vorhanden ist.
- Kopieren der Programmdateien. Bereits vorhandene veraltete Dateien werden überschrieben.
- Kopieren der AntiVir-Konfigurationsdateien. Bereits vorhandene AntiVir-Konfigurationsdateien werden beibehalten.
- Optional: Erstellen eines Links in */usr/bin*, so dass AntiVir aus allen Verzeichnissen ohne vorangestellte Pfadangabe aufgerufen werden kann.
- Optional: Installieren des residenten Wächters AntiVir Guard und des Kernel-Moduls Dazuko.
- Optional: Installieren des Gnome-Plug-Ins.
- Optional: Installieren des Avira Updaters.
- Optional: Konfigurieren eines automatischen Starts von Avira Updater und AntiVir Guard beim Systemstart.
- Optional: Installieren des Plug-Ins für Avira Security Management Center.

Installation vorbereiten

- Loggen Sie sich als ***root*** ein. Ansonsten haben Sie keine ausreichende Berechtigung für die Installation und das Skript bricht mit einer Fehlermeldung ab.
- Wechseln Sie in das Verzeichnis, in das Sie AntiVir entpackt haben, also etwa:
  `cd /tmp/antivir-server-prof-<version>`
  oder
  `cd /tmp/antivir-workstation-prof-<version>`

AntiVir installieren (Beispiel für AntiVir Server)



Avira empfiehlt und unterstützt das Kernel-Modul Dazuko3/ DazukoFS, wenn Sie den Guard von Avira AntiVir Server/ Professional v.3 benutzen wollen.

Das Installationsskript installiert auch Dazuko3, wenn es auf Ihrem System die benötigten Build-Komponenten findet.

Wenn das Skript aber keine unterstützte Linux-Kernel-Version findet, können Sie Avira AntiVir zunächst ohne Dazuko installieren. Der AntiVir Guard kann später problemlos nachinstalliert werden. Lesen Sie hierfür weiter, unter Das Kernel-Modul Dazuko – Seite 48.

▶ Geben Sie ein:
`./install`
Achten Sie auf den führenden Punkt und Schrägstrich. Ein Aufruf von "install" ohne diese Pfadangabe führt typischerweise zum Aufruf eines anderen, hier nicht zu involvierenden Kommandos und in der Folge zu Fehlermeldungen oder ungewollten Aktivitäten. Der für den Lizenztext verwendete Dateibetrachter kann typischerweise mit der Taste ***q*** verlassen werden.

↳ Das Installationsskript läuft an. Nach dem Akzeptieren der Lizenzbedingungen werden die Programmdateien kopiert. Optional übernimmt der Installer einen zuvor bereitgelegten Lizenzkey:

```
Do you agree to the license terms? [n] y

creating /usr/lib/AntiVir ... done
copying AV_SRV_PROF to /usr/lib/AntiVir/ ... done
copying LICENSE to /usr/lib/AntiVir/LICENSE-server ... done


1) installing AntiVir Core Components (Engine, Savapi and Avupdate)
copying uninstall to /usr/lib/AntiVir/ ... done
copying etc/file_list to /usr/lib/AntiVir/ ... done
.....

Enter the path to your key file: [HBEDV.KEY]
copying HBEDV.KEY to /usr/lib/AntiVir/avira.key ... done

installation of AntiVir Core Components (Engine, Savapi and Avupdate) complete
```

↳ Nachdem Sie den Pfad zur Lizenz-Datei eingeben, das Installationsskript fragt, ob Sie einen Link in */usr/bin* erstellen wollen, so dass AntiVir aus allen Verzeichnissen ohne vorangestellte Pfadangabe aufgerufen werden kann:

```
2) Configuring updates
An internet updater is available...
...
Would you like to create a link in /usr/sbin for avupdate ? [y]
```

▶ Geben Sie ***y*** ein und bestätigen Sie mit ***Enter***.

Anschließend werden Sie gefragt, ob Sie einen cron-Task für automatische Aktualisierung erstellen wollen:

```
linking /usr/sbin/avupdate-guard ... done

Would you like to setup Scanner update as cron task ? [y]
```



Der Cron-Task führt die Aktualisierung genau zu der Uhrzeit aus, zu der AntiVir installiert wurde. Wenn Sie eine andere Uhrzeit für die Aktualisierungen bevorzugen, können Sie die Vorgaben später unter /etc/cron.d/avira_updater ändern.

▶ Bestätigen Sie mit ***Enter***. Sie können diese Einstellung später wieder rückgängig machen.

↳ Dann müssen Sie das Zeitintervall für Aktualisierung wählen: täglich (d) oder alle 2 Stunden (2):

```
Please specify the interval to check.
Recommended values are daily or 2 hours.

available options: d [2]
```

▶ Geben Sie ***d*** oder ***2*** ein.

↳ Wenn Sie tägliche Aktualisierung gewählt haben, können Sie dann die Zeit bestimmen:

```
The AntiVir Updater can be set to always check for updates at a particular time of
day. This is specified in a HH:MM format (where HH is the hour and MM is the
minutes). If you do not have a permanent connection, you may set it to a time
when you are usually online.

available option: HH:MM

What time should updates be done [00:15]?
```

▶ Geben Sie ggf. die Zeit ein und bestätigen Sie mit ***Enter***.

↳ Anschließend wird gefragt, ob Sie wöchentliche Produkt-Aktualisierungen ausführen wollen:

```
Would you like to check for Guard updates once a week ? [n]
```

▶ Antworten Sie mit ***y***, wenn Sie einverstanden sind, oder drücken Sie einfach ***Enter***, wenn nicht.

↳ Anschließend wird gefragt, ob das Hauptprogramm installiert werden soll.
Wenn das Skript kein Dazuko-Modul auf Ihrem System findet, versuchtes Dazuko zu installieren:

```
3) installing main program
copying doc/avserver_en.pdf to /usr/lib/AntiVir/ ... done
copying bin/linux_glibc22/libdazuko3compat2.so to /usr/lib/AntiVir/ ... done
...
No Dazuko device found on your system
Would you like to install dazuko now ? [y]
```

▶ Antworten Sie mit ***y***, wenn Sie Dazuko installieren wollen, um den AntiVir Guard zu benutzen, und bestätigen Sie mit ***Enter.***

↳ Das Dazuko3-Paket wird installiert.

```
installing dazuko ... Available Dazuko3-Package: '3.0.0-rc4'

checking for needed build components:
    checking for C compiler cc ... found
    checking for C compiler gcc ... found
    checking for kernel sources ... found

detecting kernel version ... 2.6.18
unpacking dazuko-3.0.0-rc4_2.6.18 ... done
installing dazuko-3.0.0-rc4_2.6.18 ...

initiate dazukofs ...
done

linking /usr/lib/AntiVir/libdazuko.so to /usr/lib/AntiVir/libdazuko3compat2.so...
```

Wenn das Installationsskript Probleme zu Dazuko meldet, müssen Sie möglicherweise Ihren UNIX-Kernel neu kompilieren. Hinweise hierzu finden Sie unter Das Kernel-Modul Dazuko – Seite 48.



Es ist möglich, AntiVir zunächst ohne Kernel-Modul Dazuko zu installieren. In diesem Fall läuft er aber ohne den AntiVir Guard.

↳ Anschließend liest das Skript die Datei */etc/fstab*, um die als DazukoFS gemounteten Verzeichnisse zu prüfen. Wenn es noch kein Eintrag gibt, müssen Sie ein Verzeichnis eingeben:

```
Guard will automatically protect all directories
 which are mounted upon dazukofs filesystem.

Please specify at least one directory to be protected
by Guard to add in /etc/fstab: [/home]
```



Es gibt Dateisysteme, die nicht Dazukofs überlagert werden sollten, da die Sicherheit nicht verbessert würde, sondern im Gegenteil zu Störungen im System führen könnte. Solche Dateisysteme sind z.B. `sysfs (/sys)`, `procfs (/proc)`, `usbfs`*. Diese Dateisysteme gestatten ohnehin nicht die Erstellung von Dateien, so dass sie auch nicht gegen Malware geschützt werden müssen.*

Das beschränkte Verzeichnis "`/`*" (*`root`*) sollte nicht mit Dazukofs gemountet werden, da dies auch das Root-Verzeichnis für andere Dateisysteme sein könnte, die ebenfalls nicht mit Dazukofs gemountet werden sollten.*

"`/`*" zu mounten könnte ebenfalls gefährlich sein, weil darunter sehr wahrscheinlich schon Dateiprozesse unter / ablaufen, bevor Dazukofs gemountet wurde.Dies kann zu undefinierten Vorgänge führen, wenn später auf diese Dateien über die Dazukofs Ebene zugegriffen wird.*

▶ Geben Sie ein Verzeichnis ein, das in Echtzeit geprüft wird (z.B. `/home`) und bestätigen Sie mit ***Enter***.
Später können Sie die Liste der überwachten Verzeichnisse ändern, indem Sie die Datei */etc/fstab* editieren und sie erneut als DazukoFS mounten.

↳ Dann prüft der Installer, ob es das Quarantäne-Verzeichnis schon gibt:

```
/home/quarantine, the AVIRA Guard default quarantine directory, does not exist.
INFO: You can change the quarantine directory in /etc/avira/avguard.conf.
  and /etc/avira/avscan.conf after the installation.
Would you like to create /home/quarantine ? [y]
```

- Bestätigen Sie ggf. mit ***Enter***, um das Verzeichnis zu erstellen. Sie können später die Einstellungen in den Konfigurationsdateien ändern.
  ↳ Anschließend wird gefragt, ob das GNOME-Plug-In installiert werden soll. Es installiert die AntiVir-Ikone in der Taskleiste (- der Guard läuft; - der Guard ist inaktiv):

```
Would you like to install the AVIRA Guard GNOME plugin? [n]
```

- Geben Sie zuerst ***y*** ein und bestätigen Sie mit ***Enter***, wenn Sie das Plug-In installieren wollen, oder geben Sie ***n*** ein, wenn nicht.
  ↳ Anschließend werden Sie gefragt, ob einen Link zum *avguard* erstellt werden soll und ob der Updater beim Systemstart automatisch gestartet werden soll:

```
Would you like to create a link in /usr/sbin for avguard ?[y]
linking /usr/sbin/avguard to /usr/lib/AntiVir/avguard ... done
Please specify if boot scripts should be set up.
Set up boot scripts [y]:
```

- Bestätigen Sie mit ***Enter***.
  ↳ Der automatische Systemstart wird konfiguriert:

```
setting up boot script ... done
installation of AVIRA Guard complete
```

↳ Anschließend wird gefragt, ob AntiVir mit dem optionalen Plug-In für Avira Security Management Center installiert werden soll:

```
4) activate SMC support
The AntiVir Security Management Center (SMC) requires this feature.
Would you like to activate the SMC support? [y]
```

- Wenn Sie Avira SMC benutzen, geben Sie ***y*** ein oder bestätigen Sie mit ***Enter***.
  ↳ Das Plug-In wird installiert. Die Installation des Avira AntiVir Server/ Professional wird abgeschlossen. Sie können AntiVir Guard starten, wenn Dazuko korrekt installiert wurde:

```
Would you like to start AVIRA Guard now? [y]
Starting Avira AntiVir Server...
Starting: avguard.bin
```

↳ Sie erhalten abschließend die Bestätigung, dass die Installation erfolgreich verlaufen ist:

```
Installation of the following features complete:
    AntiVir Core Components (Engine, Savapi and Avupdate)
    AntiVir Internet Updater
    AVIRA Guard
    AntiVir SMC plugin
```

3.4 AntiVir erneut installieren oder deinstallieren

Sie können das Installationsskript jederzeit neu aufrufen. Hiermit sind folgende Vorgänge möglich:

- Nachinstallation einzelner Komponenten, z. B des AntiVir Guard oder des Avira Updater.
- Aktivierung oder Deaktivierung des automatischen Starts des Avira Updater und des AntiVir Guard.

AntiVir erneut installieren

Das Vorgehen ist für alle Fälle gleich:

✓ Stellen Sie sicher, dass der AntiVir Guard nicht läuft:
`/usr/lib/AntiVir/avguard stop`

Wechseln Sie in das temporäre Verzeichnis, in das Sie AntiVir Server:entpackt haben, also etwa:
`cd /tmp/antivir-server-prof-<version>`
or, for AntiVir Professional:
`cd /tmp/antivir-workstation-prof-<version>`Geben Sie ein:
`./install`

↳ Das Installationsskript läuft weitgehend ab wie in der Erstinstallation beschrieben (siehe AntiVir installieren – Seite 10).

▶ Ändern Sie die entsprechenden Einstellungen während der Installation.

↳ AntiVir ist mit den neuen Einstellungen installiert.

AntiVir deinstallieren

Wenn Sie Avira AntiVir Server/ Professional deinstallieren wollen, können Sie das *uninstall* Skript benutzen. Es liegt in dem temporären AntiVir-Verzeichnis. Die Syntax lautet:

```
uninstall [--product=productname] [--inf=inf-file] [--force]
[--version] [--help]
```

mit `Guard` als `productname`.

▶ Wechseln Sie in das temporäre Verzeichnis, in das Sie AntiVir entpackt haben:

`cd /usr/lib/AntiVir`

▶ Geben Sie ein:

`./uninstall --product=Guard`

↳ Das Skript deinstalliert das Produkt. Es fragt ob Sie eine Kopie der Lizenz-Datei behalten möchten; ob Sie die Konfigurationsdateien und Logdateien sichern möchten; es kann auch die cron-Tasks für den automatischen Systemstart von Guard und Scanner löschen.

- Antworten Sie mit ***y*** oder ***n*** und bestätigen Sie mit ***Enter***.
  ↳ Avira AntiVir Server/ Professional ist deinstalliert.

3.5 Anbindung an AMaViS

Das Projekt "A Mail Virus Scanner (AMaViS)" (http://www.amavis.org/) ist bereits für den Einsatz zusammen mit dem AntiVir-Scanner vorbereitet. AMaViS muss entweder nach der Installation von AntiVir installiert werden, so dass die automatische Erkennung stattfindet. Oder die Unterstützung von AntiVir muss beim Installieren von AMaViS explizit aktiviert werden, wahlweise mit den Optionen `--enable-all` oder `--enable-hbedv` für das Kommando `./configure`.



Bitte beachten Sie, dass AMaViS den Kommandozeilenscanner benutzt und diesen für jede einzelne Nachricht als separaten Prozess ausführt. Dieses Verfahren ist damit leider nicht so performant wie ein dedizierter Email-Scanner. Für Umgebungen mit höheren Anforderungen an den Durchsatz sollten Sie also den Einsatz von AntiVir MailGate oder von auf SAVAPI basierenden Produkten erwägen.



Für den Einsatz des Kommandozeilenscanners zusammen mit AMaViS ist eine Server-Lizenz erforderlich. Nur diese erlaubt es Antiviren-Scandienste für andere Rechner zu erbringen.

4 Konfiguration

Damit AntiVir Server/ Professional optimal auf Ihrem System läuft, müssen Sie AntiVir konfigurieren. Bereits im Anschluss an die Installation haben Sie die Möglichkeit, die wichtigsten Einstellungen vorzunehmen. Dabei werden Ihnen Einstellungen vorgeschlagen, die für viele Fälle sinnvoll sind. Sie können jederzeit nachträglich diese Einstellungen ändern und so AntiVir immer optimal anpassen.

Nach einer kurzen Übersicht werden Sie Schritt für Schritt in die Konfiguration eingeführt:

- Beschreibung der Konfigurationsdateien:

-Konfiguration des AntiVir Guard in avguard.conf – Seite 17

-Konfiguration des Kommandozeilenscanner in avscan.conf – Seite 26

-Scanner spezifische Konfiguration in avguard-scanner.conf – Seite 32

-Konfiguration des Avira Updater in avupdate.conf – Seite 33

- Abschließend wird in AntiVir Server/Professional testen - Seite 34 erklärt, wie Sie die korrekte Konfiguration von AntiVir prüfen.

4.1 Konfigurationsdateien

Die Konfiguration wird in vier Dateien definiert:

- *avguard.conf* definiert das Verhalten des residenten Wächters AntiVir Guard.
- *avscan.conf* definiert das Verhalten des Kommandozeilenscanners.
- *avguard-scanner.conf* definiert das Verhalten von SAVAPI3.
- *avupdate.conf* definiert das automatische Update der Software und die Protokollierung desselben.



Die Einstellungen können direkt in den Konfigurationsdateien vorgenommen werden. Sie können aber auch als Parameter in den Kommandozeilen benutzt werden und so haben sie Vorrang vor den Einstellungen in Konfigurationsdateien.

Dieser Abschnitt beschreibt den Aufbau der Konfigurationsdateien von AntiVir Server/ Professional. Diese Dateien liest AntiVir Server/ Professional beim Programmstart ein. Leerzeilen und Zeilen, die mit # beginnen, werden ignoriert.

Bei Lieferung sind Werte eingestellt, die für viele Anwendungen sinnvoll sind. Einige Einträge sind durch ein vorgestelltes # deaktiviert (auskommentiert) und können durch Entfernen des # aktiviert werden.



Wenn Sie manuell Werte in den Konfigurationsdateien ändern, müssen Sie anschließend den AntiVir Guard manuell neu starten. Erst dann werden die Änderungen wirksam.

▶ Geben Sie dafür ein:

```
/usr/lib/AntiVir/avguard restart
```

4.1.1 Konfiguration des AntiVir Guard in *avguard.conf*

Im Folgenden werden die Einträge in *avguard.conf* kurz beschrieben. Diese Einträge beeinflussen nur das Verhalten von AntiVir Server/ Professional und nicht die anderen Programme von AntiVir.

Ondemand Mgmt

Läuft als Dämon für den On-Demand Scanner:
Wenn die Option `OndemandMgmt` aktiv ist, der Guard läuft als Dämon für den On-Demand Scanner. Echtzeit-Scannen wird inaktiv. In der Voreinstellung ist diese Option deaktiviert.



Alle Optionen sind bei deaktiviertem Guard nicht aktiv. Um den On-Demand Scanner einzustellen, schauen Sie sich bitte die s *avscan.conf* Datei an.

```
OnAccessMgmt auto
```

Num Daemons

Anzahl Dämonen:
Die Anzahl der AntiVir Guard-Dämonen, die gleichzeitig laufen, kann zwischen 3 und 20 eingestellt werden. Der voreingestellte Wert 3 ist sinnvoll für kleinere Standardrechner. Für leistungsfähige Industrie-PC kann eine höhere Anzahl sinnvoll sein:

```
NumDaemons 3
```

Wenn der Wert auf 0 gesetzt wird, wird der AntiVir Guard deaktiviert.

Repair Concerning Files

Reparatur von Dateien:
Der AntiVir Guard ist in der Lage, Dateien sofort beim Zugriff zu reparieren. Schlägt dies fehl, wird der Zugriff geblockt. Hierfür muss folgende Option aktiviert werden:

Wenn `RepairConcerningFiles` aktiviert ist, reagiert AntiVir Guard auf jede Warnung mit einem Reparaturversuch der infizierten Datei. Wenn die Reparatur erfolgreich war, wird der Zugriff gewährt und keine weitere Aktion, abgesehen von der Protokollierung, ausgeführt.
Schlägt der Reparaturversuch fehl, wird der Zugriff gesperrt und die Alert Action, falls Sie eine festgelegt haben, wird ausgeführt.

```
RepairConcerningFiles
```

In der Voreinstellung ist diese Option deaktiviert.

AlertAction

Aktion bei Funden von Viren oder unerwünschten Programmen:
Wenn `RepairConcerningFiles` nicht eingestellt ist oder die Reparatur nicht möglich ist, wird der Zugriff auf die Datei gesperrt und der Vorgang protokolliert. Über folgende drei Optionen werden weitere Aktionen vom AntiVir Guard definiert:

- `none` oder `ignore`: keine weiteren Aktionen.
- `rename` oder `ren`: Umbenennen der Datei durch Anhängen der Endung *.XXX*
- `delete` oder `del`: Löschen der Datei.
- `quarantine`: Verschieben der Datei in Quarantäne, wenn eingestellt (siehe unten).

Nur eine der Optionen kann eingestellt sein, AntiVir wählt jeweils die letzte in der Konfigurationsdatei aufgeführte aus. Voreingestellt:

```
AlertAction none
```

Quarantine Directory

Wenn Sie die Option `quarantine` für `AlertAction` benutzen wollen (siehe oben), müssen Sie zuerst das Quarantäne-Verzeichnis einstellen.

Hinweis: Wenn Sie kein Quarantäne-Verzeichnis angeben, wird das folgende Verzeichnis automatisch erstellt und infizierte Dateien werden dorthin verschoben:

```
QuarantineDirectory /home/quarantine
```

Alert Conditions

Alert Actions anhand konfigurierbarer Alarmzustände:

Die auszuführenden Alert Actions lassen sich auf den gemeldeten Alarmzustand abstimmen (z.B. für verschlüsselte Dateien oder Archive, die als verdächtigt markiert wurden).

Abhängig von der einzelnen Aktion, wird auf die Warnung wie folgt reagiert:
- `ignore` - die Warnung wird ignoriert.
- `warn` - der Zustand wird als Warnung geloggt; der Zugriff wird vom Guard nicht gesperrt.
- `block` - der Zugriff wird gesperrt.
- `alert` - der Zugriff wird gesperrt; die AlertAction wird ausgeführt (höchste Priorität).

Auf jeden der folgenden Zustände kann mit diesen Aktionen reagiert werden: `ignore`, `warn`, `block` oder `alert`. Voreingestellt sind:
- `ArchiveMaxSizeAction block`
- `ArchiveMaxRecursionAction block`
- `ArchiveMaxRatioAction block`
- `ArchiveMaxCountAction block`
- `ScanIncompleteAction warn`
- `ArchiveEncryptedAction warn`
- `ArchiveMultiVolumeAction warn`
- `ArchiveUnsupportedAction warn`
- `ArchiveHeaderMalformedAction warn`
- `ArchiveBombAction block`
- `TaggedSuspiciousAction warn`
- `ArchiveProcErrorAction warn`

AccessMask

AccessMask (nur für Dazuko2):
In der Access Mask wird festgelegt, bei welchen Zugriffen der AntiVir Guard eine Datei auf Viren und unerwünschte Programme scannt:
- 1: Scannen bei Öffnen einer Datei
- 2: Scannen bei Schließen einer Datei
- 4: Scannen bei Ausführen einer Datei

Um einen Scan bei mehreren Zugriffsarten zu definieren, werden die obigen möglichen Werte für AccessMask addiert. Für Scannen bei Öffnen und Schließen einer Datei muss z. B. der Wert auf `3` gesetzt werden. Voreingestellt ist:

```
AccessMask 3
```



Bitte beachten Sie, dass AntiVir Guard nur auf diese Situationen reagieren und Dateien scannen kann, wenn das Kernel-Modul diese Ereignisse tatsächlich liefert. Nicht jedes Betriebssystem unterstützt alle Ereignisse in jeder Version des Kernels, zusätzlich können bei der Erzeugung des Kernel-Moduls einzelne Ereignisse an- oder abgewählt werden. Unabhängig von der Verwendung der anderen Ereignisse wird empfohlen, **immer auch beim Öffnen von Dateien** scannen zu lassen.

IncludePath

Überwachte Verzeichnisse (nur für Dazuko2):
Der AntiVir Guard scannt die Dateien im angegebenen Verzeichnis inklusive aller Unterverzeichnisse.

Das Dateisystem unter *\/home* ist für gewöhnlich besonders angreifbar, da dort die Daten der verschiedenen Nutzer liegen. Entsprechend ist die Voreinstellung:

```
IncludePath /home
```

Pro Eintrag ist nur ein Verzeichnis zugelassen. Mehrere Verzeichnisse können angegeben werden, allerdings jeweils als eigener Eintrag in einer separaten Zeile. Beispiel:

```
IncludePath /home
IncludePath /tmp
```



Wenn kein Verzeichnis angegeben wird, startet der AntiVir Guard nicht!



Dazuko3 ignoriert diese Option. Es ist daher angeraten, sie nicht mit **Dazuko3** verwenden, da der AntiVir Guard sonst nicht startet!

ExcludePath **Ausgeschlossene Verzeichnisse:**
Wenn Sie nicht alle Unterordner innerhalb eines durch `IncludePath` definierten Pfades schützen wollen, kann der AntiVir Guard einzelne Verzeichnisse von der Überwachung ausnehmen, z. B. ein Verzeichnis, in das temporäre Dateien von AntiVir-Komponenten gelegt werden. Eine Voreinstellung gibt es nicht.

Pro Eintrag ist nur ein Verzeichnis zugelassen (Schrägstrich am Ende hinzufügen). Mehrere Verzeichnisse können natürlich trotzdem angegeben werden, allerdings jeweils als eigener Eintrag in einer separaten Zeile. Beispiel:

```
ExcludePath /home/log/
ExcludePath /home/tmp/
```

ExcludePattern **Vom On-Access-Scannen ausgeschlossene PCRE-Muster**:
Mit dieser Option legen Sie fest, welche Dateien/Verzeichnisse vom On-Access Scannen ausgeschlossen werden sollen. Die Dateien/Verzeichnisse werden nicht gescanned, wenn ihre Namen mit dem gegeben PCRE-Muster übereinstimmen (Perl-kompatible reguläre Ausdrücke).

```
ExcludePattern [regex]
```

Sie können auch unterschiedliche PCRE-Muster gleichzeitig vom Scan ausschließen. Dazu zählen Sie alle Ausdrücke, die Sie ausschließen wollen, als Optionen in der Konfigurationsdatei auf. Beispiel:

```
ExcludePattern usr/share
ExcludePattern src/kernels
ExcludePattern usr/lib
ExcludePattern(so|h|mo|gz)$
```

Voreingestellt: `ExcludePattern NONE`..



Obwohl Dateinamen oft auf einen bestimmte Dateiart hinweisen (Auch unter UNIX), so gibt es keine technische Verbindung zwischen Dateinamen und -arten unter UNIX. Daher kann eine Sicherheitslücke entstehen, wenn bestimmte Dateien aufgrund der Dateinamen vom Scanvorgang ausgeschlossen werden.



Bitte bachten Sie, dass die Dateinamen normalisiert werden, bevor der Musterabgleich Anwendung findet. Daher können Teile des Pfadnamens ungewollt eine Übereinstimmung auslösen, wenn der Ausdruck nicht vorsichtig geschrieben wurde.



Wenn symbolische Verknüpfungen gescannt werden, werden die Dateien, auf die sie verweisen, abgeglichen.

ExcludeExt

Ausgeschlossene Dateierweiterungen:
Diese Option ermöglicht es Ihnen bestimmte Dateierweiterungen zu bestimmen, die vom On-Acess Scan ausgeschlossen werden sollen.

```
ExcludeExt [spec]
```

wenn `[spec]` eine durch Doppelpunkte getrennte Liste von Dateierweiterungen ist, z.B.: `exe:bat:com`.

Voreingestellt: `ExcludeExt NONE`

Temporary Directory

Temporäres Verzeichnis der Guard-Dateien:
Dieses Verzeichnis enthält temporäre Dateien des AntiVir Guard. Beispiel:

```
TemporaryDirectory /tmp
```

ScanMode

Konfiguration zu scannender Dateien:
Mit diesem Eintrag wird festgelegt nach welchem Verfahren bestimmt wird ob eine Datei zu scannen ist. Mögliche Werte sind:

- `extlist`: nur Dateien scannen, deren Namen mit einer bestimmten Kennung enden;
- `smart`: Dateien aufgrund sowohl ihres Namens als auch unter Einbeziehung ihres Dateityps scannen;
- `all`: Dateien unbesehen ihres Typs oder Namens immer scannen.

Voreingestellt ist, dass alle Dateien überprüft werden:

```
ScanMode all
```



Um die folgende Programmfunktion nutzen zu können, wird der Einsatz von Dazuko 2.0.0 oder höher vorausgesetzt.

ArchiveScan

Überwachte Archive:
Der AntiVir Guard scannt zusätzlich komprimierte Archive beim Zugriff, abhängig von den Einstellungen in `ArchiveMaxSize`, `ArchiveMaxRecursion` und `ArchiveMaxRatio`. Hierfür muss folgende Option aktiviert werden:

```
ArchiveScan yes
```

In der Voreinstellung ist diese Option aktiviert, um die Sicherheit möglichst hoch zu halten.

MailboxScan

Überwachte Mailboxen:
Wenn `ArchiveScan` aktiv ist, kann der AntiVir Guard zusätzlich Mailboxen beim Zugriff scannen. Hierfür muss folgende Option aktiviert werden:

```
MailboxScan yes
```

In der Voreinstellung ist diese Option aktiviert.

ArchiveMaxSize **Maximale Archivgröße:**
Mit diesem Eintrag wird der Scanvorgang auf Dateien beschränkt, die im unkomprimierten Zustand kleiner als `ArchiveMaxSize` (bytes, KB, MB, GB) sind. Bei einem Wert von 0 findet keine Beschränkung statt. Voreingestellt ist ca. 1 GByte:

```
ArchiveMaxSize 1 GB
```

ArchiveMaxRecursion **Rekursionstiefe für Archive:**
Wenn rekursiv gepackte Archive gescannt werden, kann die Rekursionstiefe auf `ArchiveMaxRecursion` beschränkt werden. Bei einem Wert von 0 findet keine Beschränkung statt. Voreingestellt:

```
ArchiveMaxRecursion 20
```

Archive MaxRatio **Dekompressionsfaktor für Archive:**
Mit diesem Eintrag wird der Scanvorgang auf Dateien beschränkt, die einen vorgegebenen Dekompressionsfaktor nicht überschreiten. Diese Maßnahme schützt vor so genannten "Mailbomben", die beim Dekomprimieren unerwartet viel Speicherplatz belegen würden. Bei einem Wert von 0 findet keine Beschränkung statt. Voreingestellt:

```
ArchiveMaxRatio 150
```

Archive MaxCount **Anzahl Dateien innerhalb eines Archivs:**
Das Scannen von Archiven wird auf die vorgegebene Anzahl von Dateien innerhalb eines Rekursionsschrittes beschränkt. Bei einem Wert von 0 findet keine Beschränkung statt. Es ist kein Wert voreingestellt.

```
ArchiveMaxCount 0
```



Das Scannen des Archivs kann beschleunigt werden, indem Sie manuell folgende Einstellungen vornehmen:

```
ARCHIVE_MAX_RECURSION 1
ARCHIVE_MAX_COUNT 10
ARCHIVE_MAX_SIZE 1000KB
```

Die Zuverlässigkeit des Scans wird dadurch nicht beeinflusst.

Anzahl Scanner-Warnungen :
MaxReportsPerFile Die maximale Anzahl der Warnmeldungen, die pro gescannter Datei ausgegeben werden. Für gewöhnlich wirkt sich dies nur auf Archivscans aus. Diese Option kann verwendet werden, damit der Scanner keine Denial-of-Service-Angriffe auslöst, die von speziell erstellten Archiven generiert werden und andernsfalls Millionen von Warnmeldungen hervorrufen würden. Der Wert 0 bedeutet, dass die Anzahl nicht beschränkt ist.

```
MaxReportsPerFile 100
```

SendSNMPTraps **SNMP-Traps Konfiguration**:
SNMP Traps können dazu genutzt werden, den Status des Systems und der Netzwerkdienste zu überwachen. Sowohl On-Demand als auch On-Access-Scanner unterstützen dieses Protokoll und versenden SNMP-Traps (einfache Textnachrichten), um Systemüberwachungstools über den aktuellen Status des Scanners, Lizenzfragen, Viruswarnungen und den Aktualisierungsstatus zu informieren. Diese Meldungen werden geloggt.

Um SNMP Traps einzuschalten:

```
SendSNMPTraps yes
```

Voreingestellt: disabled (`no`).

SNMP VerbosityLevel

Ausführlichkeitsgrad der SNMP Traps:

`SNMPVerbosityLevel [notice|information|warning|error|alert|snmp]`

Bestimmt für welche Angelegenheiten Traps gesendet werden sollen, wenn Dateien gescannt werden. Voreingestellt: nur SNMP-spezifische Warnungen und wichtige Statusinformationen werden versendet (`snmp` level):

`SNMPVerbosityLevel snmp`

Abgesehen von `snmp`, werden Syslog Level unterstützt. Zum Beispiel:

`SNMPVerbosityLevel information`

Die folgenden Meldungen werden via SNMP versendet: Meldungen mit der Priorität "information", "warning", "error", "alert" PLUS die SNMP-spezifischen Meldungen.



Das `SNMPVerbosityLevel` beeinflusst nicht den Syslog Ausführlichkeitsgrad oder umgekehrt.

SNMPRecipient

Geben Sie einen Hostnamen oder eine IP Addresse an, um den Empfänger der SNMP Traps zu bestimmen:

`SNMPRecipient <hostname | IP address>`

Voreingestellt: `SNMPRecipient localhost`

External Program



Bitte benutzen Sie diese Funktion mit Vorsicht! Prüfen Sie die Vollständigkeit des externen Programms und beachten Sie, dass Angreifer, durch schlaue Dateinamen (die Leerzeichen, Kommandos u.ä. enthalten), Ihr externes Programm ausnutzen können.

Start eines externen Prozesses bei Fund verdächtiger Dateien:
Wird ein Virus bzw. unerwünschtes Programm gefunden, kann der AntiVir Guard einen externen Prozess starten. Dieser kann eine über die Fähigkeiten des AntiVir Guard hinausgehende Benachrichtigung veranlassen oder eine sonstige Nachbereitung übernehmen.

Möglich sind z. B. der Versand einer SMS, der Anruf eines Verantwortlichen, die Anzeige eines Dialogfensters am lokalen Bildschirm oder auch an einem entfernt stehenden Windows-Rechner, das Speichern der vorliegenden Daten in einem anderen Format oder in einer Datenbank.

Vor dem Start werden Platzhalter (mit % beginnende Sequenzen) durch die konkreten Daten des auslösenden Ereignisses ersetzt. Dies ermöglicht eine differenzierte Behandlung und die Anpassung an lokale Gegebenheiten.

Die folgende Aufstellung listet die unterstützten Platzhalter und ihre Ersetzung auf:

Option	Funktion
`%h`	Verzeichnis, in dem sich die Datei befindet, kann Sonderzeichen enthalten
`%f`	Dateiname ohne Verzeichnis-Anteil, kann Sonderzeichen enthalten
`%p`	Vollständiger Dateiname inklusive Verzeichnis (gleich wie %h/%f), kann Sonderzeichen enthalten

Option	Funktion
%U	UID der Datei (numerische Account-Bezeichnung des Eigentümers)
%G	GID der Datei (numerische Account-Bezeichnung der UNIX-Gruppe)
%s	Dateigröße
%m	Zugriffsrechte der Datei (oktal)
%De	Typ des auslösenden Ereignisses
%DF	Dateisystem/Partition, auf dem/der sich die Datei befindet (hexadezimal)
%Dp	PID des zugreifenden Prozesses
%Du	UID, unter der der zugreifende Prozess läuft
%Df	Flags der ausgeführten Datei-Operation (hexadezimal)
%Dm	Zugriffsmodus der ausgeführten Datei-Operation (hexadezimal)
%Sn	Bezeichnung des gefundenen Virus bzw. der gefundenen unerwünschten Software
%Sa	Zusatz-Informationen (falls verfügbar)
%SU	Alert URL



Einige der übergebenen Parameter werden nicht von AntiVir geprüft, sondern aus den Datei-Eigenschaften übernommen und an den gestarteten Prozess weitergegeben. Sie sollten deshalb vor der weiteren Verarbeitung geprüft werden.

```
ExternalProgram /bin/sh /usr/lib/AntiVir/popup_message.sh [%Sn] %p
```

Voreingestellt: `none`



Es gibt keine Statusmeldungen über das Aufrufen der externen Programme.

Email-Nachrichten:

EmailTo

AntiVir Guard kann Emails verschicken, wenn ein Virus oder unerwünschtes Programm entdeckt wurde. Eine Voreinstellung gibt es nicht. Um Emails zu verschicken muss ein Adressat angegeben werden, z.B.:

```
EmailTo root@localhost
```

Suppress Notification Below

Email-Benachrichtigungen nach Dringlichkeit filtern:

Mit dieser Einstellung kann gesteuert werden, dass Benachrichtigungen an die mit `EmailTo` konfigurierte Adresse nicht verschickt werden, wenn sie eine geringere als die vorgegebene Dringlichkeitsstufe haben. Es werden nur Benachrichtigungen verschickt,

die der angegebenen oder einer höheren Stufe zugeordnet sind. Syntax:
`SuppressNotificationBelow scanner <level>`

Mögliche Werte für `<level>` (in aufsteigender Folge) sind `notice`, `information`, `warning`, `error` und `alert`. In der Voreinstellung werden keine Benachrichtigungen verworfen.

```
SuppressNotificationBelow scanner warning
```

LogFile **Logdatei:**
Alle wichtigen Operationen von AntiVir werden über den *syslog*-Dämon protokolliert. Zusätzlich kann eine Logdatei geschrieben werden. Eine Voreinstellung gibt es nicht. Damit die Logdatei geschrieben werden kann, muss der volle Pfad zur Datei angegeben werden, z. B:

```
LogFile /var/log/avguard.log
```

Syslog... **Syslog-Einstellung:**
Für alle wichtigen Operationen gibt AntiVir Server/ Professional Meldungen an den *syslog*-Dämon. Zusätzlich kann spezifiziert werden, welche Facility und Priorität diesen Meldungen mitgegeben wird. Voreingestellt sind:

```
SyslogFacility user
SyslogPriority notice
```

Das Einstellen der `SyslogPriority` legt fest, dass alle Meldungen, die von gleicher poder höher Priorität sind als die angegebene, geloggt werden. Dementsprechend erhalten Sie mit dem `Priority Warning` alle Meldungen, die mit `Alert`, `Error` or `Warning` gekennzeichnet sind. Da `Info` eine niedrigere Priorität hat als `Warning` werden Sie keine `Info` Nachrichten erhalten.

Diese Werte gelten auch, wenn `LogFile` deaktiviert ist.

DetectPrefixes **Erkennung weiterer unerwünschter Programme:**
Neben Viren existieren noch andere Arten von Software, die Schaden anrichten können oder aus anderem Grund unerwünscht sind. Die Erkennung dieser Software kann mit folgenden Optionen aktiviert werden. Die Erkennung von Viren ist nicht optional und kann nicht deaktiviert werden.

- `adspy` - Software, die Werbung einblendet oder Software, die persönliche Daten des Anwenders häufig ohne dessen Wissen oder Zustimmung an Dritte versendet und daher möglicherweise unerwünscht ist.
- `appl` - Eine Applikation, deren Nutzung mit einem Risiko verbunden sein kann oder die von fragwürdiger Herkunft ist.
- `bdc` - Die Steuersoftware von Backdoors. BDCs sind normalerweise harmlos.
- `dial` - Ein Dial-Up-Programm für kostenpflichtige Verbindungen, die riesige Rechnungen verursachen können.
- `game` - Computerspiele, die eigentlich dem Computer nicht schaden.
- `hiddenext` - Ausführbare Dateien, die ihre wahre Dateiendung in verdächtiger Weise verschleiern.
- `joke` - Dateien mit Witzprogrammen.
- `pck`- Dateien, die mit einem ungewöhnlichen Laufzeitpacker komprimiert wurden.
- `phish` - Gefälschte E-Mails, die den Benutzer nach persönliche Informationen fragen, wie z.B. Benutzerkonto, Passwort, Online-Banking-Daten u.s.w.
- `spr` - Software, die die Sicherheit Ihres Systems beeinträchtigen, nicht gewünschte Programmaktivitäten auslösen, Ihre Privatsphäre verletzen oder Ihr Benutzerverhalten ausspähen kann.
- `alltypes` - Alle oben genannten Malware-Arten.

Syntax: Sie können eine Liste von Prefixes eingeben, indem Sie die Parameter durch Leerzeichen oder Doppelpunkt trennen.

```
DetectPrefixes <type>[=<bool>] <type>[=<bool>] ...
```

Beispiel:

```
DetectPrefixes adspy=yes appl=no bdc=yes dial=yes game=no
hiddenext=no joke=no pck=no phish=yes spr=no
```

HeuristicsMacro

Makroviren-Heuristik:
Aktiviert die Heuristik für Makroviren in Dokumenten. In der Voreinstellung ist diese Option aktiviert.

```
HeuristicsMacro yes
```

HeuristicsLevel

Win32-Datei-Heuristik:
Stellt die Erkennungsstufe der Win32-Datei-Heuristik ein. Zulässige Werte sind `0` (aus), `1` (niedrig), `2` (mittel) und `3` (hoch). Voreingestellt:

```
HeuristicsLevel 1
```

GUISupport

Unterstützung durch grafische Benutzeroberfläche (GUI):
Dieser Eintrag muss aktiviert sein, damit AntiVir mit der GUI von Avira SMC kommunizieren kann. Folgende Parameter müssen eingetragen sein:

```
GuiSupport     yes
GuiCAFile      /usr/lib/AntiVir/gui/cert/cacert.pem
GuiCertFile    /usr/lib/AntiVir/gui/cert/server.pem
GuiCertPass    antivir_default
```

Wenn diese Parameter nicht vorhanden oder falsch sind, steht das GUI-Support nicht zur Verfügung. Mögliche Fehler werden in der log-Datei protokolliert.

ActiveLockFile

Lockfile des Guards:
Sie müssen den vollständigen Pfad zu Guard-Lockfile eingeben, sodass andere Software den Guard auf Ihrem Computer identifizieren. Diese Datei wird auch vom Gnome-Plug-In benutzt.

```
ActiveLockFile /var/lock/LCK..avguard
```

4.1.2 Konfiguration des Kommandozeilenscanner in *avscan.conf*

Beginnend mit AntiVir Server/ Professional v.3 wurde eine neue Konfigurationsdatei eingeführt: *avscan.conf*. Diese Datei enthält spezielle Konfigurationsoptionen für den Kommandozeilenscanner (AntiVir CLS).

Repair Concerning Files

Reparatur von Dateien:
Der Kommandozeilenscanner (CLS) ist in der Lage, Dateien zu reparieren. Schlägt dies fehl, wird der Zugriff geblockt. Hierfür muss folgende Option aktiviert werden:

```
RepairConcerningFiles yes
```

In der Voreinstellung ist diese Option deaktiviert.

AlertAction

Aktion bei Funden von Viren oder unerwünschten Programmen:
Wenn `RepairConcerningFiles` nicht eingestellt ist oder die Reparatur nicht möglich ist, wird der Zugriff auf die Datei gesperrt und der Vorgang protokolliert. Über folgende drei Optionen werden weitere Aktionen vom AntiVir CLS definiert:

- `none` oder `ignore`: keine weiteren Aktionen.
- `rename` oder `ren`: Umbenennen der Datei durch Anhängen der Endung *.XXX*

- `delete` oder `del`: Löschen der Datei.
- `quarantine`: Verschieben der Datei in das Quarantäneverzeichnis, wenn angegeben (siehe unten).

Nur eine der Optionen kann eingestellt sein, AntiVir wählt jeweils die letzte in der Konfigurationsdatei aufgeführte aus. Voreingestellt:

```
AlertAction none
```

Quarantine Directory

Wenn Sie die Option `quarantine` für `AlertAction` benutzen wollen (siehe oben), müssen Sie zuerst das Quarantäne-Verzeichnis angeben. Voreingestellt:

```
QuarantineDirectory /home/quarantine
```

ExcludePattern

Vom On-Demand-Scannen ausgeschlossene PCRE-Muster:
Der AntiVir CLS kann einzelne PCRE-Patterns (Perl-compatible regular expressions) von der Überwachung ausnehmen.

```
ExcludePattern [regex]
```

Sie können auch unterschiedliche PCRE-Muster gleichzeitig vom Scan ausschließen. Dazu zählen Sie alle Ausdrücke, die Sie ausschließen wollen, als Optionen in der Konfigurationsdatei auf. Beispiel:

```
ExcludePattern usr/share
ExcludePattern src/kernels
ExcludePattern usr/lib
ExcludePattern(so|h|mo|gz)$
```

In der Voreinstellung ist diese Option deaktiviert.

`ExcludePattern NONE`.



Obwohl Dateinamen oft auf einen bestimmte Dateiart hinweisen (Auch unter UNIX), so gibt es keine technische Verbindung zwischen Dateinamen und -arten unter UNIX. Daher kann eine Sicherheitslücke entstehen, wenn bestimmte Dateien aufgrund der Dateinamen vom Scanvorgang ausgeschlossen werden.



Wenn symbolische Verknüpfungen gescannt werden, werden die Dateien, auf die sie verweisen, abgeglichen.

ExcludeExt

Ausgeschlossene Dateierweiterungen:
Diese Option ermöglicht es Ihnen bestimmte Dateierweiterungen zu bestimmen, die vom On-Demand Scan ausgeschlossen werden sollen.

```
ExcludeExt [spec]
```

wenn `[spec]` eine durch Doppelpunkte getrennte Liste von Dateierweiterungen ist, z.B.: `exe:bat:com`.

Voreingestellt: `ExcludeExt NONE`

Temporary Directory

Temporäres Verzeichnis der CLS-Dateien:
Dieses Verzeichnis enthält temporäre Dateien des AntiVir CLS. Beispiel:

```
TemporaryDirectory /tmp
```

Hinweis: Bitte achten Sie darauf, dass in diesem Verzeichnis ausreichend Speicherplatz, d.h. mindestens 4 GB, zur Verfügung stehen.

FollowSymlink **Die Reaktion von CLS auf Symlinks:**
AntiVir Kommandozeilenscanner folgt standardmäßig Symlinks. Sie können aber dieses Verhalten deaktivieren.

```
FollowSymlink yes
```

ScanMode **Konfiguration zu scannender Dateien:**
Mit diesem Eintrag wird festgelegt nach welchem Verfahren bestimmt wird ob eine Datei zu scannen ist. Mögliche Werte sind:

- `extlist`: nur Dateien scannen, deren Namen mit einer bestimmten Kennung enden;
- `smart`: Dateien aufgrund sowohl ihres Namens als auch unter Einbeziehung ihres Dateityps scannen;
- `all`: Dateien unbesehen ihres Typs oder Namens immer scannen.

Voreingestellt ist:

```
ScanMode smart
```

ArchiveScan **Überwachte Archive:**
Der AntiVir CLS scannt zusätzlich komprimierte Archive, abhängig von den Einstellungen in `ArchiveMaxSize`, `ArchiveMaxRecursion` und `ArchiveMaxRatio`. Hierfür muss folgende Option aktiviert werden:

```
ArchiveScan yes
```

In der Voreinstellung ist diese Option aktiviert, um die Sicherheit möglichst hoch zu halten.

MailboxScan **Überwachte Mailboxen:**
Wenn `ArchiveScan` aktiv ist, kann der AntiVir CLS zusätzlich Mailboxen scannen. Hierfür muss folgende Option aktiviert werden:

```
MailboxScan yes
```

In der Voreinstellung ist diese Option aktiviert.

ArchiveMax Size **Maximale Archivgröße:**
Mit diesem Eintrag wird der Scanvorgang auf Dateien beschränkt, die im unkomprimierten Zustand kleiner als `ArchiveMaxSize` (bytes, KB, MB, GB) sind. Bei einem Wert von 0 findet keine Beschränkung statt. Voreingestellt ist 1 GByte:

```
ArchiveMaxSize 1GB
```

ArchiveMax Recursion **Rekursionstiefe für Archive:**
Wenn rekursiv gepackte Archive gescannt werden, kann die Rekursionstiefe auf `ArchiveMaxRecursion` beschränkt werden. Bei einem Wert von 0 findet keine Beschränkung statt. Voreingestellt:

```
ArchiveMaxRecursion 20
```

Archive MaxRatio **Dekompressionsfaktor für Archive:**
Mit diesem Eintrag wird der Scanvorgang auf Dateien beschränkt, die einen vorgegebenen Dekompressionsfaktor nicht überschreiten. Diese Maßnahme schützt vor so genannten "Mailbomben", die beim Dekomprimieren unerwartet viel Speicherplatz belegen würden. Bei einem Wert von 0 findet keine Beschränkung statt. Voreingestellt:

ArchiveMaxRatio 150

Archive MaxCount

Anzahl Dateien innerhalb eines Archivs:
Das Scannen von Archiven wird auf die vorgegebene Anzahl von Dateien innerhalb eines Rekursionsschrittes beschränkt. Bei einem Wert von 0 findet keine Beschränkung statt. Es ist kein Wert voreingestellt.

ArchiveMaxCount 0



Das Scannen des Archivs kann beschleunigt werden, indem Sie manuell folgende Einstellungen vornehmen:

```
ARCHIVE_MAX_RECURSION 1
ARCHIVE_MAX_COUNT 10
ARCHIVE_MAX_SIZE 1000KB
```

Die Zuverlässigkeit des Scans wird dadurch nicht beeinflusst.

SendSNMPTraps

SNMP-Traps Konfiguration:
SNMP Traps können dazu genutzt werden, den Status des Systems und der Netzwerkdienste zu überwachen. Sowohl On-Demand als auch On-Access-Scanner unterstützen dieses Protokoll und versenden SNMP-Traps (einfache Textnachrichten), um Systemüberwachungstools über den aktuellen Status des Scanners, Lizenzfragen, Viruswarnungen und den Aktualisierungsstatus zu informieren. Diese Meldungen werden geloggt.

Um SNMP Traps einzuschalten:

SendSNMPTraps yes

Voreingestellt: disabled (no).

SNMP VerbosityLevel

Ausführlichkeitsgrad der SNMP Traps:

SNMPVerbosityLevel [notice|information|warning|error|alert|snmp]

Bestimmt für welche Angelegenheiten Traps gesendet werden sollen, wenn Dateien gescannt werden. Voreingestellt: nur SNMP-spezifische Warnungen und wichtige Statusinformationen werden versendet (snmp level):

SNMPVerbosityLevel snmp

Abgesehen von snmp, werden Syslog Level unterstützt. Zum Beispiel:

SNMPVerbosityLevel information

Die folgenden Meldungen werden via SNMP versendet: Meldungen mit der Priorität "information", "warning", "error", "alert" PLUS die SNMP-spezifischen Meldungen.



Das SNMPVerbosityLevel beeinflusst nicht den Syslog Ausführlichkeitsgrad oder umgekehrt.

SNMPRecipient

Geben Sie einen Hostnamen oder eine IP Addresse an, um den Empfänger der SNMP Traps zu bestimmen:

SNMPRecipient <hostname | IP address>

Voreingestellt: SNMPRecipient localhost

External Program



Bitte benutzen Sie diese Funktion mit Vorsicht! Prüfen Sie die Vollständigkeit des externen Programms und beachten Sie, dass Angreifer, durch schlaue Dateinamen (die Leerzeichen, Kommandos u.ä. enthalten), Ihr externes Programm ausnutzen können.

Start eines externen Prozesses bei Fund verdächtiger Dateien:
Wird ein Virus bzw. unerwünschtes Programm gefunden, kann der AntiVir Guard einen externen Prozess starten. Dieser kann eine über die Fähigkeiten des AntiVir Guard hinausgehende Benachrichtigung veranlassen oder eine sonstige Nachbereitung übernehmen.

Möglich sind z. B. der Versand einer SMS, der Anruf eines Verantwortlichen, die Anzeige eines Dialogfensters am lokalen Bildschirm oder auch an einem entfernt stehenden Windows-Rechner, das Speichern der vorliegenden Daten in einem anderen Format oder in einer Datenbank.

Vor dem Start werden Platzhalter (mit % beginnende Sequenzen) durch die konkreten Daten des auslösenden Ereignisses ersetzt. Dies ermöglicht eine differenzierte Behandlung und die Anpassung an lokale Gegebenheiten.

Die folgende Aufstellung listet die unterstützten Platzhalter und ihre Ersetzung auf:

Option	Funktion
`%h`	Verzeichnis, in dem sich die Datei befindet, kann Sonderzeichen enthalten
`%f`	Dateiname ohne Verzeichnis-Anteil, kann Sonderzeichen enthalten
`%p`	Vollständiger Dateiname inklusive Verzeichnis (gleich wie %h/%f), kann Sonderzeichen enthalten
`%U`	UID der Datei (numerische Account-Bezeichnung des Eigentümers)
`%G`	GID der Datei (numerische Account-Bezeichnung der UNIX-Gruppe)
`%s`	Dateigröße
`%m`	Zugriffsrechte der Datei (oktal)
`%De`	Typ des auslösenden Ereignisses
`%DF`	Dateisystem/Partition, auf dem/der sich die Datei befindet (hexadezimal)
`%Dp`	PID des zugreifenden Prozesses
`%Du`	UID, unter der der zugreifende Prozess läuft
`%Df`	Flags der ausgeführten Datei-Operation (hexadezimal)
`%Dm`	Zugriffsmodus der ausgeführten Datei-Operation (hexadezimal)
`%Sn`	Bezeichnung des gefundenen Virus bzw. der gefundenen unerwünschten Software
`%Sa`	Zusatz-Informationen (falls verfügbar)
`%SU`	Alert URL



Einige der übergebenen Parameter werden nicht von AntiVir geprüft, sondern aus den Datei-Eigenschaften übernommen und an den gestarteten Prozess weitergegeben. Sie sollten deshalb vor der weiteren Verarbeitung geprüft werden.

```
ExternalProgram /bin/sh /usr/lib/AntiVir/popup_message.sh [%Sn] %p
```

LogFile

Logdatei:
Alle wichtigen Operationen von AntiVir werden über den *syslog*-Dämon protokolliert. Zusätzlich kann eine Logdatei geschrieben werden. Eine Voreinstellung gibt es nicht. Damit die Logdatei geschrieben werden kann, muss der volle Pfad zur Datei angegeben werden, z. B:

```
LogFile /var/log/avscan.log
```

Syslog...

Syslog-Einstellung:
Für alle wichtigen Operationen gibt AntiVir Server/ Professional Meldungen an den *syslog*-Dämon. Zusätzlich kann spezifiziert werden, welche Facility und Priorität diesen Meldungen mitgegeben wird. Voreingestellt sind:

```
SyslogFacility user
SyslogPriority notice
```

Diese Werte gelten auch, wenn `LogFile` deaktiviert ist.

DetectPrefixes

Erkennung weiterer unerwünschter Programme:
Neben Viren existieren noch andere Arten von Software, die Schaden anrichten können oder aus anderem Grund unerwünscht sind. Die Erkennung dieser Software kann mit folgenden Optionen aktiviert werden. Die Erkennung von Viren ist nicht optional und kann nicht deaktiviert werden.

- `adspy` - Software, die Werbung einblendet oder Software, die persönliche Daten des Anwenders häufig ohne dessen Wissen oder Zustimmung an Dritte versendet und daher möglicherweise unerwünscht ist.
- `appl` - Eine Applikation, deren Nutzung mit einem Risiko verbunden sein kann oder die von fragwürdiger Herkunft ist.
- `bdc` - Die Steuersoftware von Backdoors. BDCs sind normalerweise harmlos.
- `dial` - Ein Dial-Up-Programm für kostenpflichtige Verbindungen, die riesige Rechnungen verursachen können.
- `game` - Computerspiele, die eigentlich dem Computer nicht schaden.
- `hiddenext` - Ausführbare Dateien, die ihre wahre Dateiendung in verdächtiger Weise verschleiern.
- `joke` - Dateien mit Witzprogrammen.
- `pck`- Dateien, die mit einem ungewöhnlichen Laufzeitpacker komprimiert wurden.
- `phish` - Gefälschte E-Mails, die den Benutzer nach persönliche Informationen fragen, wie z.B. Benutzerkonto, Passwort, Online-Banking-Daten u.s.w.
- `spr` - Software, die die Sicherheit Ihres Systems beeinträchtigen, nicht gewünschte Programmaktivitäten auslösen, Ihre Privatsphäre verletzen oder Ihr Benutzerverhalten ausspähen kann.
- `alltypes` - Alle oben genannten Malware-Arten.

Syntax: Sie können eine Liste von Prefixes eingeben, indem Sie die Parameter durch Leerzeichen oder Doppelpunkt trennen.

```
DetectPrefixes <type>[=<bool>] <type>[=<bool>] ...
```

Beispiel:

```
DetectPrefixes adspy=yes appl=no bdc=yes dial=yes game=no
hiddenext=no joke=no pck=no phish=yes spr=no
```

Heuristics Macro

Makroviren-Heuristik:
Aktiviert die Heuristik für Makroviren in Dokumenten. In der Voreinstellung ist diese Option aktiviert.

```
HeuristicsMacro yes
```

Heuristics Level

Win32-Datei-Heuristik:
Stellt die Erkennungsstufe der Win32-Datei-Heuristik ein. Zulässige Werte sind `0` (aus), `1` (niedrig), `2` (mittel) und `3` (hoch). Voreingestellt:

```
HeuristicsLevel 1
```

GUISupport

Unterstützung durch grafische Benutzeroberfläche (GUI):
Dieser Eintrag muss aktiviert sein, damit AntiVir mit der GUI von Avira SMC kommunizieren kann. Folgende Parameter müssen eingetragen sein:

```
GuiSupport     yes
GuiCAFile      /usr/lib/AntiVir/gui/cert/cacert.pem
GuiCertFile    /usr/lib/AntiVir/gui/cert/server.pem
GuiCertPass    antivir_default
```

Wenn diese Parameter nicht vorhanden oder falsch sind, steht das GUI-Support nicht zur Verfügung. Mögliche Fehler werden in der log-Datei protokolliert.

4.1.3 Scanner spezifische Konfiguration in *avguard-scanner.conf*

Beginnend mit AntiVir Server/ Professional v.3 wurde eine neue Konfigurationsdatei eingeführt: *avguard-scanner.conf*. Diese Datei enthält spezielle Konfigurationsoptionen für das neue Scanner-Backend. Die Optionen in dieser Datei brauchen nur in einigen wenigen Ausnahmefällen geändert zu werden.

SyslogFacility

Syslog-einstellung:

```
SyslogFacility user
```

ReportLevel

Der Scanner kann auf verschiedene Protokollstufen eingestellt werden:

- 0 – Fehler
- 1 – Fehler und Alarme
- 2 – Fehler, Alarme und Warnungen
- 3 – Fehler, Alarme, Warnungen und Debug-Meldungen

Ein „Alarm“ enthält Informationen über potentiell schädlichen Code.

Standardeinstellung:

```
ReportLevel 0
```

LogFileName

Der Pfad der Scanner-Logdatei.

```
LogFileName NONE
```

AlertURL

Option um Informationen über Malware via Internet herunterzuladen. Es werden zur Zeit folgende URLs unterstützt:
Deutsch: http://www.avira.com/de/threats?q=%1
Englisch: http://www.avira.com/en/threats?q=%1

```
AlertURL:<URL>
```

4.1.4 Konfiguration des Avira Updater in *avupdate.conf*

Aktualisierungen stellen sicher, dass die Komponenten von Avira AntiVir Server/ Professional (Guard, Scanner, VDF und Engine), die für den Schutz vor Viren und unerwünschten Programmen sorgen, stets auf dem neuesten Stand sind.

Mit Avira Updater können Sie die Avira-Software auf Ihrem Rechner mithilfe von Avira-Update-Servern aktualisieren.

Um den Aktualisierungsvorgang zu konfigurieren, verwenden Sie die Optionen in */etc/avira/avupdate.conf*, die weiter unten beschrieben sind. Alle Parameter in *avupdate.conf* können dem Updater in der Befehlszeile übergeben werden. Ein Beispiel:

– Parameter in avupdate.conf:

```
temp-dir=/tmp
```

– Befehlszeile:

```
/usr/lib/AntiVir/guard/avupdate-guard --temp-dir=/tmp
```

internet-srvs — Die Liste der Internet-Update-Server.

```
internet-srvs=http://dl1.pro.antivir.de, http://
dl2.pro.antivir.de, http://dl3.pro.antivir.de
```

master-file — Die master.idx-Datei.

```
master-file=/idx/master.idx
```

install-dir — Das Installationsverzeichnis für aktualisierte Produktdateien.

```
install-dir=/usr/lib/AntiVir/guard
```

temp-dir — Temporäres Verzeichnis für heruntergeladene Aktualisierungsdateien.

```
temp-dir=/tmp/avira_update/guard
```

HTTP proxy settings

proxy... — Falls Sie einen http Proxy Server für die Internetupdates nutzen, müssen Sie Folgendes eingeben:

```
proxy-host=
proxy-port=
proxy-username=
proxy-password=
```

E-Mail-Aktualisierungsberichte einstellen

Alle Berichte über AntiVir-Aktualisierungen werden an die E-Mail-Adressen gesendet, die in *avupdate.conf* angegeben sind:

smtp... — Authentifizierung der smtp-Verbindung. Aktivieren Sie die Option `auth-method` und geben Sie den smtp-Server, den Port, den Benutzer und das Passwort an.

```
mailer=[smtp | sendmail]
```

```
auth-method=password
smtp-user=<Ihr_Benutzername>
smtp-password=<Ihr_Passwort>
```

```
smtp-server=<Servername>
smtp-port=<Port>
```

notify-when — E-Mail-Benachrichtigungen können auf drei Werte eingestellt werden:

- 0 – Es werden keine E-Mail-Benachrichtigungen gesendet.
- 1 – E-Mail-Benachrichtigungen werden in folgenden Fällen gesendet: „Aktualisierung erfolgreich“, „Aktualisierung nicht erfolgreich“ und „Auf dem neuesten Stand“.
- 2 – Eine E-Mail-Benachrichtigung wird nur bei „Aktualisierung nicht erfolgreich“ gesendet.
- 3 - Eine Email-Benachrichtigung wird nur bei „Aktualisierung erfolgreich“ verschickt.

```
notify-when=3
```

email-to — Der Empfänger der E-Mail-Benachrichtigungen.

```
email-to=root@localhost
```

Logdatei-Einstellungen

log — Geben Sie den vollständigen Pfad und Namen der Datei an, in die AntiVir Updater seine Log-Meldungen schreibt.

```
log=/var/log/avupdate.log
```

log-append — Die Logdatei wird standardmäßig überschrieben. Sie können diese Option benutzen, um die Log-Meldungen am Ende des Logdatei zu schreiben.

```
log-append
```

4.2 AntiVir Server/ Professional testen

Nach Abschluss der Installation und der Konfiguration können Sie die Funktionsfähigkeit von AntiVir Server/ Professional testen. Hierfür ist ein Testvirus erhältlich. Dieser richtet keinerlei Schaden an, löst aber bei einem intakten Virenschutz auf Ihrem Rechner eine Reaktion des Programms aus.

AntiVir Guard mit Testvirus testen

- Wählen Sie in Ihrem Web-Browser die Adresse http://www.eicar.org.
- Informieren Sie sich auf dieser Webseite über den verfügbaren Testvirus *eicar.com*.
- Laden Sie den Testvirus auf Ihren Rechner (z.B. unter `/TEST`) herunter.
- Auf Dazuko3-Systemen, mounten Sie das Verzeichnis, in dem Sie den Testvirus gespeichert haben:
  `mount -t dazukofs /TEST /TEST`
- Versuchen Sie es, die Testvirus-Datei via shell Befehl “less” zu öffnen.
  ↳ AntiVir Guard blockiert den Zugriff.

AntiVir Kommandozeilenscanner mit Testvirus testen

- Wählen Sie in Ihrem Web-Browser die Adresse http://www.eicar.org.
- Informieren Sie sich auf dieser Webseite über den verfügbaren Testvirus *eicar.com*.
- Laden Sie den Testvirus auf Ihren Rechner (z.B. unter `/TEST`) herunter.

- Geben Sie ein:
  `avscan /TEST`
  ↳ AntiVir CLS zeigt eine Warnung an und fragt nach weiteren Aktionen.

Eventuelle Fehler suchen

Wenn der AntiVir Guard nicht die erwarteten Meldungen ausgibt oder Aktionen ausführt, müssen Sie Ihre Konfiguration überprüfen.

- Prüfen Sie, ob der AntiVir Guard läuft. Geben Sie ein:
  `/usr/lib/AntiVir/avguard status`
- Starten Sie den AntiVir Guard, falls nötig.
- Wenn Sie AntiVir Guard in Kombination mit Dazukofs verwenden, stellen Sie sicher, dass die Verzeichnisstruktur, die sie mit OnAccess Schutz versehen wollen, mit Dazukofs gemountet ist.
  Nutzen Sie den `mount` Befehl, um eine Liste aller gemounteten Verzeichnisse/ Partitionen aufzurufen.
- Wenn Sie AntiVir Guard in Kombination mit Dazuko2 verwenden, stellen Sie sicher, dass die Verzeichnisstruktur, die sie mit OnAccess Schutz versehen wollen, mithilfe der `IncludePath` Option festgelegt wurde. Stellen Sie außerdem sicher, dass der Wert von `AccessMask` nicht auf 0 gesetzt ist, da der AntiVir Guard sonst nicht startet.
- Prüfen Sie Meldungen des AntiVir Guard an Ihre Logdatei oder an *syslog*, um den Fehler einzugrenzen.

5 Bedienung

Nach Abschluss der Installation und der Konfiguration ist die laufende Überwachung Ihres Systems durch AntiVir Guard gewährleistet. Im laufenden Betrieb werden unter Umständen gelegentliche Änderungen der Konfiguration sinnvoll sein, die Sie gemäß Konfiguration – Seite 17 vornehmen.

Dennoch kann in bestimmten Fällen eine gezielte manuelle Suche nach Viren bzw. unerwünschten Programmen notwendig sein. Hierfür steht der AntiVir Kommandozeilenscanner zur Verfügung. Dieses Programm ermöglicht mit vielen Optionen spezifische Suchläufe.

Der AntiVir Kommandozeilenscanner kann in Skripte eingebunden werden und auch über Cron-Jobs regelmäßig ausgeführt werden. Dem fortgeschrittenen UNIX -Nutzer bieten sich damit zahllose Möglichkeiten einer optimal abgestimmten Überwachung seines Systems.

Dieses Kapitel ist unterteilt in folgende Abschnitte:

- In Echtzeit Suche mit AntiVir Guard – Seite 36 erhalten Sie einen Überblick über sämtliche Optionen des AntiVir Guard.
- In Exit-Codes – Seite 43 erhalten Sie einen Überblick über sämtliche Optionen des AntiVir Kommandozeilenscanners sowie exemplarische Anwendungen des Kommandozeilenscanners.
- In Vorgehen bei Fund eines Virus/unerwünschten Programms – Seite 45 geben wir einige Hinweise auf das, was Sie tun sollten, wenn AntiVir seine Arbeit verrichtet hat.

5.1 Echtzeit Suche mit AntiVir Guard

Aufruf

Um den AntiVir Guard zu starten, stoppen oder neustarten, oder den Status zu zeigen:

```
avguard {start|stop|status|restart}
```

Beispiel:

Wenn Guard bereits läuft, wird der Befehl

```
avguard status
```

die folgende Meldung anzeigen:

"Status: avguard.bin running."

Um den Guard mit bestimmten Optionen zu benutzen:

```
avguard [Option]
```

Optionen

Folgende Optionen stehen – auch kombinierbar – für den AntiVir Guard zur Verfügung:

Option	**Funktion**
`--alert-action=<spec>`	Aktion bei Funden von Viren oder unerwünschten Programmen. Siehe auch AlertAction – Seite 18 `--alert-action=quarantine`

--archive-max-count=<spec>	Legt eine Anzahl an in Archiven enthaltenen Dateien fest. Mit Erreichen der festgelegten Zahl, beendet der Scanner den Scan-Prozess.
--archive-max-ratio=<spec>	Schließt in Archiven enthaltene Dateien vom Scan aus, wenn sie einen Dekompressionsfaktor jenseits des angegebenen Wertes haben.
--archive-max-ratio-action=	Aktion bei oben genannter Bedingung. Kann auf `ignore`, `warn`, `block` oder `alert` festgesetzt werden.
--archive-max-recursion=<spec>	Schließt in Archiven enthaltene Dateien vom Scan aus, wenn ihre Schachtelungstiefe größer als der angegebene Wert ist.
--archive-max-recursion-action=	Aktion bei oben genannter Bedingung. Kann auf `ignore`, `warn`, `block` oder `alert` festgesetzt werden.
--archive-max-size=<spec>	Schließt in Archiven enthaltene Dateien vom Scan aus, wenn sie beim Dekomprimieren größer als der angegebene Wert werden.
--archive-max-size-action=	Aktion bei oben genannter Bedingung. Kann auf `ignore`, `warn`, `block` oder `alert` festgesetzt werden.
--archive-encrypted-action=	Aktion bei verschlüsselten Archiven. Kann auf `ignore`, `warn`, `block` oder `alert` festgesetzt werden.
--archive-multivolume-action=	Aktion bei Multivolume Archiven.Kann auf `ignore`, `warn`, `block` oder `alert` festgesetzt werden.
--archive-unsupported-action=	Aktion bei einem nicht unterstützten Archiv. Kann auf `ignore`, `warn`, `block` oder `alert` festgesetzt werden.
--archive-header-malformed-action=	Aktion bei einem fehlerhaft formatierten Header. Kann auf `ignore`, `warn`, `block` oder `alert` festgesetzt werden.
--archive-bomb-action=	Aktion ausgelöst durch ein Bombenarchiv. Kann auf `ignore`, `warn`, `block` oder `alert` festgesetzt werden.
--archive-procerror-action=	Aktion ausgelöst durch einen Verarbeitungsfehler. Kann auf `ignore`, `warn`, `block` oder `alert` festgesetzt werden.

`--config`	Zeigt ein Beispiel der Konfigurationsdatei an.
`-C <configuration-file>`	Benutzt eine andere Konfigurationsdatei statt der voreingestellten.

`--detect-prefixes=<spec>`	Aktiviert die Erkennung von unerwünschten Programmen, die keine Viren sind. Sie können eine Liste von Prefixes eingeben, indem Sie die Parameter durch Leerzeichen oder Doppelpunkt trennen.
	`--detect-prefixes='adspy=yes: joke=no:spr:bdc'`
	Um alle Typen gleichzeitig zu aktivieren:
	`--detect-prefixes=alltypes`
	Siehe auch DetectPrefixes – Seite 25.

`--exclude-ext=<ext>{:<ext>}`	Gibt an, dass die genannten Erweiterungen vom Scannen ausgeschlossen sind. Beispiel: `--exclude-ext=exe:com:bat` Hinweis: Beim Scannen symbolischer Verknüfungen, werden die Dateien, auf die sie verweisen, gescannt.
`--exclude-path=<dir>`	Schließt das angegebene Verzeichnis vom Scan aus.
`--exclude-pattern=<spec>`	Gibt an, was vom Scannen ausgeschlossen wird. Lässt sich mittels einer durch Doppelpunkte getrennten Liste von Perl-kompatiblen regulären Ausdrücken (PCRE) festlegen. Beispiel: `--exclude-pattern="^/tmp/TEST/"` Warnung: *Bitte beachten Sie, dass die Dateinamen normalisiert werden, bevor der Musterabgleich Anwendung findet. Daher können Teile des Pfadnamens ungewollt eine Übereinstimmung auslösen, wenn der Ausdruck nicht vorsichtig geschrieben wurde.* Hinweis: *Wenn symbolische Verknüpfungen gescannt werden, werden die Dateien, auf die sie verweisen, abgeglichen.*
`--help`	Syntax und Optionen für *avguard.bin* werden ausgegeben. (auch: `-h` oder `-?`)
`--heur-level=<int>`	Stellt die Erkennungsstufe der Win32-Datei-Heuristik ein. Stufe 0: aus Stufe 1: niedrig Stufe 2: mittel Stufe 3: hoch

--heur-macro[=<bool>]	(De)Aktiviert die Heuristik für Makroviren in Dokumenten.
--log-email=<addr>	Sendet einen Report über den Scan-Durchlauf per Email an die angegebene Adresse. Akzeptiert eine durch Leerzeichen getrennte E-Mails-Liste.
--scan-in-archive[=<bool>]	Auch Inhalte von gepackten Archiven werden gescannt. Voreingestellt.
--scan-in-mbox[=<bool>]	Auch Inhalte von Mailbox-Ordnern werden gescannt. Voreingestellt.
--scan-incomplete-action=	Aktion bei unvollständigen Scans. Kann auf `ignore`, `warn`, `block` oder `alert` festgesetzt werden.
--scan-mode=<spec>	Stellt das Verfahren ein, nach dem bestimmt wird, ob eine Datei zu scannen ist. `ScanMode {all|smart|ext}`
--send-snmp-traps=yes|no	Aktiviert/deaktiviert SNMP Traps. Voreingestellt: `no` (keine)
--snmp-verbosity-level=<level>	Bestimmt den Ausführlichkeitsgrad der SNMP Traps; neben SNMP unterstützt es auch Syslog Ebenen `notice|information|warning|error|alert`. Voreingestellt: Nur SNMP-spezifische und wichtige Statusinformationen werden versendet.
--snmp-recipient=<localhost| ip address>	Der String beinhaltet den Localhost oder die IP Adresse, die für die Einstellung der SNMP-Traps-Empfänger notwendig ist.
--temp-dir=<dir>	AntiVir legt seine temporären Dateien in `<dir>` ab.
--version	Die Version von AntiVir wird angezeigt.

5.2 On-Demand Suche mit AntiVir Kommandozeilenscanner

Aufruf

Um den AntiVir Kommandozeilenscanner (CLS) zu starten:

```
avscan [Option] [Verzeichnis [...]]
```

Wenn kein Verzeichnis angegeben wird, scannt der AntiVir Kommandozeilenscanner das aktuelle Verzeichnis.

Wenn gezielt Dateien in einem Verzeichnis durchsucht werden sollen, wird der AntiVir Kommandozeilenscanner aufgerufen über

```
avscan [Option] [Verzeichnis][Dateiname]
```

Optionen

Folgende Optionen stehen – auch kombinierbar – für den AntiVir Kommandozeilenscanner zur Verfügung. Alle andere Strings, die keine Option sind, werden als Datei oder Verzeichnis behandelt (voreingestellt ist es, nur die erste Ebene des Verzeichnis zu scannen):

Option	**Function**
`--alert-action=<spec>`	Aktion bei Funden von Viren oder unerwünschten Programmen. Siehe auch AlertAction – Seite 26 `--alert-action=quarantine`
`--archive-max-count=<N>`	Legt eine Anzahl an in Archiven enthaltenen Dateien fest. Mit Erreichen der festgelegten Zahl, beendet der Scanner den Scan-Prozess.
`--archive-max-ratio=<N>`	Schließt in Archiven enthaltene Dateien vom Scan aus, wenn sie einen Dekompressionsfaktor jenseits des angegebenen Wertes haben.
`--archive-max-recursion=<N>`	Schließt in Archiven enthaltene Dateien vom Scan aus, wenn ihre Schachtelungstiefe größer als der angegebene Wert ist.
`--archive-max-size=<N>`	Schließt in Archiven enthaltene Dateien vom Scan aus, wenn sie beim Dekomprimieren größer als der angegebene Wert werden.
`--batch`	Aktiviert den "batch"-Modus: Wenn diese Option aktiviert ist, läuft der Scan im nicht-interaktiven Batch-Modus. D.h. dass alle Aktionen anhand der vorhandenen Konfigurationsdatei und der Befehlszeilen-Einstellungen ausgeführt werden. Der Benutzer wird nicht aufgefordert, Aktionen auszuführen oder zu bestätigen. Hinweis: Wenn Sie als vorzunehmende Alert Action `delete` festgesetzt haben, wird sie im "batch"-Modus für Dateien, die nur als verdächtig angesehen werden, automatisch auf `quarantine` zurückgesetzt.
`--config`	Zeigt einen Beispiel der Konfigurationsdatei an.
`-C <configuration-file>`	Eine andere Konfigurationsdatei benutzen.

`--detect-prefixes=<spec>`	Aktiviert die Erkennung von unerwünschten Programmen, die keine Viren sind. Sie können eine Liste von Prefixes eingeben, indem Sie die Parameter durch Leerzeichen oder Doppelpunkt trennen. `--detect-prefixes='adspy=yes:joke=no:spr:bdc'` Um alle Typen gleichzeitig zu aktivieren: `--detect-prefixes=alltypes` Siehe auch DetectPrefixes – Seite 31.
`-e`	Die betroffenen Dateien reparieren, wenn möglich.
`--exclude-ext=<ext>{:<ext>}`	Gibt an, dass die genannten Erweiterungen vom Scannen ausgeschlossen sind. Beispiel: `--exclude-ext=exe:com:bat` Hinweis: Beim Scannen symbolischer Verknüfungen, werden die Dateien, auf die sie verweisen, gescannt.
`--exclude-pattern=<spec>`	Gibt an, was vom Scannen ausgeschlossen wird. Lässt sich mittels einer durch Doppelpunkte getrennten Liste von Perl-kompatiblen regulären Ausdrücken (PCRE) festlegen. Beispiel: `--exclude-pattern="^/tmp/TEST/"` Warnung: *Bitte beachten Sie, dass die Dateinamen normalisiert werden, bevor der Musterabgleich Anwendung findet. Daher können Teile des Pfadnamens ungewollt eine Übereinstimmung auslösen, wenn der Ausdruck nicht vorsichtig geschrieben wurde.* Hinweis: *Wenn symbolische Verknüpfungen gescannt werden, werden die Dateien, auf die sie verweisen, abgeglichen.*
`--follow-symlink[=yes|no]`	AntiVir Kommandozeilenscanner folgt standardmäßig Symlinks. Sie können aber dieses Verhalten deaktivieren.
`--help`	Syntax und Optionen für *avscan.bin* werden ausgegeben. (auch: `-h` oder `-?`)
`--heur-level=<int>`	Stellt die Erkennungsstufe der Win32-Datei-Heuristik ein. Stufe 0: aus Stufe 1: niedrig Stufe 2: mittel Stufe 3: hoch

--heur-macro[=<yes|no>]	(De)Aktiviert die Heuristik für Makroviren in Dokumenten.
--log-file=<filename>	Name und Pfad der Logfile.
--max-runtime=<seconds>	Mit dieser Option kann beim normalen oder geplanten Scannen eine Laufzeitbegrenzung eingestellt werden. Wird diese überschritten, wird der Prozess nach Abschluss der laufenden Teilaufgabe (Scan-/Datenbankaktion) angehalten.
--query-results	Im Planungsmodus fragt AvScan die Datenbank ab, anstatt die Dateien zu scannen. Hinweis: *Verwenden Sie diese Option nicht zeitgleich mit --scan-scheduled-files.*
--query-alerts	Im Planungsmodus fragt AvScan die Datenbank ab und zeigt nur Dateien an, die eine Virenmeldung ausgelöst haben. Hinweis: *Verwenden Sie diese Option nicht zeitgleich mit --scan-scheduled-files.*
--query-warnings	Im Planungsmodus fragt AvScan die Datenbank ab und zeigt nur Dateien an, die eine Virenwarnung ausgelöst haben. Hinweis: *Verwenden Sie diese Option nicht zeitgleich mit --scan-scheduled-files.*
--query-statistics	Im Planungsmodus fragt AvScan die Datenbank ab und zeigt Statistiken des letzten geplanten Scans und der gesamten Scanergebnisse an. Hinweis: *Verwenden Sie diese Option nicht zeitgleich mit --scan-scheduled-files.*
--quarantine-dir=<dir>	Name und Pfad der Quarantäne-Datei.
-s	Aktiviert rekursives Scannen der Unterverzeichnissen in dem angegebenen Verzeichnis.
--scan-continue-file=<filename>	Im Planungsmodus nimmt der Scanner planmäßige Scans, die abgebrochen wurde, wieder auf.
--scan-in-archive[=<bool>]	Auch Inhalte von gepackten Archiven werden gescannt. Voreingestellt.
--scan-in-mbox[=<bool>]	Auch Inhalte von Mailbox-Ordnern werden gescannt. Voreingestellt.
--scan-incomplete-action=	Aktion bei unvollständigen Scans. Kann auf `ignore`, `warn`, `block` oder `alert` festgesetzt werden.

--scan-mode=<spec>	Stellt das Verfahren ein, nach dem bestimmt wird, ob eine Datei zu scannen ist. ScanMode {all|smart|ext}
--schedule-scan=yes|no	Aktiviert den Scanplaner indem die Datenbank aktualisiert anstatt ein direkter Scan durchgeführt führt. Voreingestellt: no
--send-snmp-traps=yes|no	Aktiviert/deaktiviert SNMP Traps. Voreingestellt: no (keine)
--snmp-verbosity-level=<level>	Bestimmt den Ausführlichkeitsgrad der SNMP Traps; neben SNMP unterstützt es auch Syslog Ebenen notice|information|warning|error|alert. Voreingestellt: Nur SNMP-spezifische und wichtige Statusinformationen werden versendet.
--scan-scheduled-files	Startet den Arbeitsprozess, um den geplanten Scan durchzuführen. Beschränkt auf den Root-User. Hinweis: *Verwenden Sie diese Option nicht zeitgleich mit --query-results, --query-alerts, --query-warnings or --query-statistics.*.
--temp=<dir>	AntiVir legt seine temporären Dateien in <dir> ab.
-v --verbose	Schaltet den ausführlichen Modus ein. Diese Option sollte nur in Ausnahmefällen ausgewählt werden, z.B. nach einer Viruswarnung oder -entfernung.
--version	Die Version von AntiVir wird angezeigt.

Exit-Codes

Der AntiVir Kommandozeilenscanner gibt nach der Ausführung Exit-Codes zurück. Diese können von fortgeschrittenen UNIX-Nutzern verwendet werden, um eigene Skripte zu erstellen.

Exit-Code	**Bedeutung**
0	Normales Programmende: kein Virus bzw. unerwünschtes Programm, kein Fehler.
1	Betroffene Datei gefunden.
3	Verdächtige Datei gefunden.
4	Warnungen wurden gemeldet.
249	Scanprozess unvollständig.
250	Scanprozess konnte nicht initialisiert werden.
251	avguard-Dämon unzugänglich.

Exit-Code	Bedeutung
252	avguard-Dämon läuft nicht.
253	Fehler beim Vorbereiten des On-Demand Scannen.
254	Konfigurationsfehler (ungültiger Parameter in Kommandozeilen oder in Konfigurationsdatei).
255	Interner Fehler.

Beispiel: Kompletten Suchlauf durchführen

Nach der Installation ist es sinnvoll, einen kompletten Suchlauf über das Dateisystem durchzuführen. Ein solcher Suchlauf enthält sinnvollerweise folgende Optionen:

`--scan-mode=all`	Scannt alle Dateien
`--detect-prefixes=alltypes`	Erkennt alle Arten von verdächtigen und unerwünschten Dateien
`-s`	Scannt alle Unterverzeichnisse
`--scan-in-archive`	Scannt auch gepackte Dateien

▶ Geben Sie ein:

```
avscan --scan-mode=all --detect-prefixes=alltypes -s
 --scan-in-archive /
```

Beispiel: Teilsuchlauf durchführen

In der Regel ist es ausreichend, diejenigen Verzeichnisse zu überprüfen, die ein- und ausgehende Daten enthalten (Mailbox, Internet, Text-Verzeichnis). Solche Daten liegen meist im Verzeichnis */var*.

Sind auf dem UNIX-System DOS-Partitionen vorhanden und gemountet, sollten diese auch geprüft werden.

Hier sind folgende Optionen sinnvoll:

`--scan-mode=all`	Scannt alle Dateien
`-s`	Scannt alle Unterverzeichnisse
`--scan-in-archive`	Scannt auch gepackte Dateien

Wenn Ihre DOS-Partitionen z. B. unter */mnt* und Ihre ein- und ausgehenden Daten unter */var* liegen:

▶ Geben Sie ein:

```
avscan --scan-mode=all -s --scan-in-archive /var /mnt
```

Beispiel: Betroffene Dateien löschen

Avira AntiVir Server/ Professional kann Dateien löschen, die Viren oder unerwünschte Programme enthalten. Optional kann AntiVir vorher versuchen, die Dateien zu reparieren.

Beim Löschen werden die Dateien vollständig gelöscht. Sie lassen sich deshalb auch mit Reparatur-Tools nicht wiederherstellen.

Hier sind folgende Optionen sinnvoll:

`--scan-mode=all`	Scannt alle Dateien
`--alert-action=delete`	Löscht betroffene Dateien
`-e --alert-action=delete`	Versucht, betroffene Dateien zu reparieren und löscht irreparable Dateien



In den nachfolgenden Beispielen werden Dateien umgewandelt oder gelöscht. Dabei kann wertvoller Datenbestand verloren gehen.

Wenn Sie alle betroffenen Dateien in */home/myhome* löschen wollen (auf Zugriffsrechte achten!):

▶ Geben Sie ein:
`avscan --scan-mode=all --alert-action=delete /home/myhome`

Wenn Sie betroffene Dateien in */home/myhome* reparieren und irreparable Dateien löschen wollen:

▶ Geben Sie ein:
`avscan --scan-mode=all -e --alert-action=delete /home/myhome`

5.3 Vorgehen bei Fund eines Virus/unerwünschten Programms

Avira AntiVir Server/ Professional hat bei richtiger Konfiguration alle wichtigen Aufgaben auf Ihrem Rechner bereits automatisch erledigt:

- Die betroffene Datei wurde repariert oder zumindest gesperrt.
- Wenn eine Reparatur nicht möglich war, wurde der Zugriff auf die Datei blockiert und die Datei, je nach Konfiguration, zusätzlich umbenannt oder verschoben. Die Gefahr einer Weitergabe des Virus oder unerwünschten Programms ist damit gebannt.

Folgende Schritte sollten Sie auf jeden Fall durchführen:

▶ Versuchen Sie zu ermitteln, auf welche Weise der Virus oder das unerwünschte Programm "eingeschleppt" wurde.

▶ Führen Sie gezielte Prüfungen an möglicherweise betroffenen Datenträgern durch.

▶ Informieren Sie Kollegen, Vorgesetzte oder Geschäftspartner.

▶ Informieren Sie Ihren Systemverantwortlichen, Ihren Viren- oder Datenschutzbeauftragten.

Verdächtige Dateien an Avira GmbH schicken

▶ Senden Sie uns bitte Viren und unerwünschte Programme, die von unseren Produkten noch nicht erkannt oder entfernt werden können, zu. Das Gleiche gilt für sonstige verdächtige Dateien. Senden Sie uns den Virus oder das unerwünschte Programm gepackt (PGP, gzip, WinZIP, PKZip, Arj) im Anhang einer Email an virus@avira.com.



Verwenden Sie beim Packen das Passwort ***virus***. Die Datei kann dann nicht von eventuellen Virenscannern in den Email-Gateways gelöscht werden.

6 Aktualisierungen

Mit Avira Updater können Sie die Avira-Software auf Ihren Rechnern mithilfe von Avira-Update-Servern aktualisieren. Das Programm kann entweder durch Bearbeiten der Konfigurationsdatei (siehe Konfiguration des Avira Updater in avupdate.conf – Seite 33) oder über Parameter in der Befehlszeile konfiguriert werden.

Es wird empfohlen, den Updater als ***root*** auszuführen. Wenn der Updater nicht als ***root*** ausgeführt wird, fehlen ihm die notwendigen Berechtigungen zum Neustart der AntiVir-Dämonen, und der Neustart muss manuell als ***root*** durchgeführt werden.

Dies hat den Vorteil, dass alle laufenden Prozesse von AntiVir-Dämonen (z. B. Scanner, Engine, Guard) automatisch mit den neuesten Antivirendateien aktualisiert werden, ohne die laufenden Prüfprozesse zu unterbrechen. Auf diese Weise ist sichergestellt, dass alle Dateien geprüft werden.

6.1 Internet-Aktualisierungen

Manuell

Wenn Sie Avira AntiVir Server/ Professional oder einige seiner Komponenten aktualisieren möchten:

▶ Verwenden Sie den folgenden Befehl:

```
/usr/lib/AntiVir/avupdate --product=[Produkt]
```

Als `[Produkt]` können Sie Folgendes eingeben:

- `Scanner` – (empfohlen) der Scanner, die Engine und die VDF-Dateien werden aktualisiert.
- `Guard` – vollständige Aktualisierung (Guard, Scanner, Engine und VDF-Dateien).

Wenn Sie nur nach einer neuen AntiVir-Version suchen möchten, ohne AntiVir zu aktualisieren:

▶ Verwenden Sie den folgenden Befehl:

```
/usr/lib/AntiVir/guard/avupdate-guard --check --pro-
duct=[Produkt]
```

Die Werte für `[Produkt]` sind die gleichen wie im obigen Beispiel.

Automatische Aktualisierungen mit dem Cron-Dämon

Regelmäßige Aktualisierungen werden mit dem Cron-Dämon durchgeführt.

Die entsprechenden Einstellungen in der Datei */etc/crontab* **sind bereits vorhanden, wenn** Sie, während der Avira AntiVir Server/ Professional-Installation mit dem *install*-Skript, die Frage, ob AntiVir Updater installiert und automatisch gestartet werden soll, mit `Ja` beantwortet haben.

Weitere Informationen über den Cron-Dämon finden Sie in Ihrer UNIX-Dokumentation.

So können Sie die Einstellungen für automatische Aktualisierungen in der crontab-Datei manuell festlegen oder ändern:

▶ Fügen Sie der Datei */etc/crontab* den gewünschten Eintrag hinzu oder bearbeiten Sie ihn (siehe folgendes Beispiel).

Beispiel: Um die Aktualisierung stündlich (immer um *:23) durchzuführen, geben Sie den folgenden Befehl ein:

```
23 * * * * root /usr/lib/AntiVir/avupdate --product=[Produkt]
```

Als `[Produkt]` können Sie Folgendes eingeben:

- `Scanner` – (empfohlen) der Scanner, die Engine und die VDF-Dateien werden aktualisiert.
- `Guard` – vollständige Aktualisierung (Guard, Scanner, Engine und VDF-Dateien).

▶ Starten Sie den Aktualisierungsprozess, um die Einstellungen zu überprüfen:

```
/usr/lib/AntiVir/avupdate --product=[Produkt]
```

Die Werte für `[Produkt]` sind die gleichen wie im obigen Beispiel.

↳ War die Aktualisierung erfolgreich, wird ein Bericht in die Logdatei */var/log/avupdate.log* geschrieben.

7 Das Kernel-Modul Dazuko

Das Kernel-Modul Dazuko ist auf allen Plattformen erforderlich, wenn die Funktionalität des AntiVir Guard benutzt werden soll. Es ist möglich, AntiVir zunächst ohne Kernel-Modul Dazuko zu installieren. In diesem Fall läuft AntiVir ohne den AntiVir Guard.



Avira empfiehlt und unterstützt das Kernel-Modul Dazuko3/ DazukoFS, wenn Sie den Guard von Avira AntiVir Server/ Professional (Unix) v.3 benutzen wollen.

Das Installationsskript installiert auch Dazuko3, wenn es auf Ihrem System die benötigten Build-Komponenten findet:

-C compiler cc,
-C compiler gcc,
-Kernel-Sourcen (Kernel-Versionen 2.6.18, 2.6.20, 2.6.22, 2.6.24, 2.6.26 oder 2.6.27).

Wenn Sie aber dazuko2 benutzen wollen, finden Sie einige Anleitungen in diesem Kapitel.

Das Modul müssen Sie selber kompilieren, denn Ihrem UNIX-Kernel und Dazuko müssen die gleichen Quelldateien zugrunde liegen. Nur so ist sichergestellt, dass Dazuko auf die gleichen Systemfunktionen wie der UNIX-Kernel zugreifen kann.



Wenn der Lieferant Ihrer Distribution bereits ein exakt zu Ihrem Kernel passendes Modul beigelegt hat:

▶ Stellen Sie fest, unter welchem Namen das Modul auf der Festplatte gespeichert wurde (bei der späteren Installation des AntiVir Guard wird diese Information benötigt). Verwenden Sie dafür z. B. den folgenden Befehl:

```
find /lib/modules/`uname -r` -name 'dazuko*'
```



Das Installationspaket enthält für SunOS (Sparc und i386) ein binäres Modul, so dass Sie dieses auf dieser Plattform nicht selbst erstellen müssen.

Im Folgenden wird das Vorgehen so beschrieben, dass Sie auch ohne Expertenkenntnisse zum Ziel kommen. Dennoch sind Kenntnisse in der Kompilierung des UNIX-Kernels nützlich, insbesondere wenn Fehler auftreten. Weitere Informationen hierzu erhalten Sie unter http://www.tldp.org/HOWTO/Kernel-HOWTO.html

7.1 Dazuko kompilieren

✓ Stellen Sie sicher, dass sich der Quellcode für den UNIX-Kernel in */usr/src/linux* befindet. Falls nicht, installieren Sie ihn nach. Informationen dazu finden Sie in der Dokumentation Ihrer UNIX-Distribution.

✓ Stellen Sie sicher, dass sich die Programme zur Kompilierung eines Kernels (z. B. gcc) auf Ihrem Rechner befinden. Bei einer UNIX-Standardinstallation ist dies der Fall. Falls nicht, installieren Sie die benötigten Programmpakete nach. Informationen dazu finden Sie in der Dokumentation Ihrer UNIX-Distribution.

✓ Ihr UNIX-Kernel muss auf dem Quellcode in */usr/src/linux* basieren. In den meisten Fällen, insbesondere nach einer Neuinstallation von UNIX, sollte dies der Fall sein.

Absolute Sicherheit hierüber können Sie allerdings nur gewinnen, indem Sie den auf dem Computer eingesetzten Kernel aus genau diesen Quellen neu kompilieren.



Bei Unsicherheiten über den Stand Ihres UNIX-Kernels können Sie dennoch die Installation fortführen. Schlimmstenfalls gelingt später zur Laufzeit die Integration von Dazuko in Ihren UNIX-Kernel nicht, so dass der Start des AntiVir Guard fehlschlägt. In diesem Fall erhalten Sie eine entsprechende Meldung und können die Situation danach bereinigen.

- Wechseln Sie in das temporäre Verzeichnis, in das Sie Dazuko entpackt haben, also z. B.:
  `cd /tmp/antivir-server-prof-<version>/contrib/dazuko/dazuko-<version>`
- Lassen Sie das Skript *configure* die Konfiguration Ihres Rechners überprüfen und unter Einbeziehung vorgefundener Details eine entsprechende Anleitung zur weiteren Übersetzung der Software erstellen:
  `./configure`
- Kompilieren Sie Dazuko mit:
  `make`
- Optional: Prüfen Sie, ob das gerade erstellte Modul mit dem auf dem Rechner laufenden Kernel zusammenarbeitet:
  `make test`
  - ↳ Sie erhalten je nach verwendetem Betriebssystem eine Datei *dazuko.o* oder *dazuko.ko* im temporären Verzeichnis. Die Pfadangabe zu dieser Datei wird später vom AntiVir-Installationsskript benötigt

Weitere aktuelle Informationen zu Dazuko erhalten Sie auf der Webseite http://www.dazuko.org. Distributionsspezifische Details sind oft schon in den FAQ ausgeführt.

7.2 Bekannte Probleme mit DazukoFS

DazukoFS mounten

Sie müssen DazuoFS gleich beim Startup mounten, via */etc/fstab,* um höhere Sicherheit zu gewährleisten. Es ist nicht zu empfehlen, ein gemountete DazukoFS zu unmounten.

Weitere Informationen erhalten Sie unter:
http://dazuko.dnsalias.org/files/README-dazukofs

Mounten via DazukoFS

Sie sollten Wechseldatenträger, wie z.B. USB-Sticks und CD-ROMs, automatisch mounten. Sonst:
- Mounten Sie die Datenträger nicht unter DazukoFS, werden sie nicht geprüft.
- Mounten Sie die Datenträger unter DazukoFS, können Sie diese nicht mehr unmounten, ohne Unmount des ganzen DazukoFS (und es könnte zum Abbruch einiger Anwendungen führen).

Symlinks beim On-Access Scannen

Bitte beachten Sie noch: Wenn Sie ein Verzeichnis via DazukoFS mounten und es enthält eine Datei (z.B. *datei.a*), die ein Symlink zu einer anderen nicht unter DazukoFS gemounteten Datei (z.B. *datei.b*) ist, dann wird der Zugriff auf *datei.a* immer erlaubt; *datei.b* wird nicht gescannt, weil nicht via DazukoFS gemountet.

Nicht unterstützte Systemaufrufe

DazukoFS unterstützt derzeit keine `sendfile()` Systemaufrufe.
Auf Grund dessen kann es zu Problemen kommen, wenn Sie DazukoFS zusammen mit anderen Anwendungen verwenden, die mit `sendfile()` arbeiten, wie z.B. Apache Server.

Wenn Sie DazukoFS zum Schutz des Basisverzeichnisses eines Apache Servers verwenden möchten, fügen Sie die folgende Zeile in die *httpd.conf* ein:

```
<Directory "/var/www">
EnableSendfile Off
</Directory>
```

Dadurch wird verhindert, dass Apache den `sendfile()` Systemaufruf verwendet.

DazukoFS unterstützt ebenfalls keine `mmap()` Systemaufrufe. Daher kann es zu Problemen (im schlimmsten Fall Datenverlust) kommen, wenn eine Applikation Memory Mapping verwendet.

8 Service

8.1 Support

Support-Service

Auf unserer Webseite http://www.avira.de erhalten Sie alle Informationen zu unserem umfangreichen Support-Service.

Die Kompetenz und Erfahrung unserer Entwickler stehen Ihnen hier zur Verfügung. Die Experten der Avira GmbH beantworten Ihre Fragen und helfen bei kniffligen technischen Problemen weiter.

Während der ersten 30 Tage nach Erwerb einer Lizenz haben Sie die Möglichkeit, den AntiVir Installationssupport in Anspruch zu nehmen, telefonisch, per Email oder per Online-Formular.

Darüber hinaus empfehlen wir Ihnen optional den Erwerb unseres AntiVir Classic Supports, mit dem Sie bei auftretenden technischen Problemen unsere Fachleute während der Geschäftszeiten kontaktieren und zu Rate ziehen können. Pro Jahr berechnen wir Ihnen für diesen Service, in dem auch der Virenbereinigungs- und Hoax-Support eingeschlossen sind, zwanzig Prozent des Listenpreises Ihres jeweils erworbenen AntiVir-Programms.

Der ebenfalls optional verfügbare AntiVir Premium Support bietet Ihnen über den Leistungsumfang des AntiVir Classic Supports hinaus genügend Spielraum, auch bei Notfällen außerhalb der Geschäftszeiten jederzeit einen kompetenten Ansprechpartner zu erreichen. Bei Virenalarm wird auf Wunsch eine SMS-Benachrichtigung auf Ihr Mobiltelefon gesendet.

Forum FAQ

Bevor Sie unsere Hotline anrufen, empfehlen wir, dass Sie unser Benutzerforum unter: http://forum.antivir.de, sowie FAQ section auf unserer Webseite besuchen.
Ihre Fragen wurden vielleicht schon von einem anderen Benutzer beantwortet und im Forum gepostet.

Email-Support

Support über Email erhalten Sie über http://www.avira.de.

8.2 Online-Shop

Sie wollen unsere Produkte bequem per Mausklick einkaufen?

Im Online-Shop der Avira GmbH können Sie unter http://www.avira.de schnell und sicher Lizenzen erwerben, verlängern oder erweitern. Der Online-Shop führt Sie Schritt für Schritt durch das Bestell-Menü. Ein multilinguales Customer-Care-Center informiert Sie über Bestellprozesse, Zahlungsabwicklungen und Auslieferung. Wiederverkäufer können auf Rechnung bestellen und ein Reseller-Panel nutzen.

8.3 Kontakt

Postadresse

Avira GmbH
Lindauer Strasse 21
D-88069 Tettnang
Deutschland

Internet Allgemeine Informationen zu uns und unseren Produkten erhalten Sie auf unserer Homepage http://www.avira.de.

9 Anhang

9.1 Glossar

Begriff	Erklärung
Backdoor-Steuerprogramme (BDC)	Um Daten zu stehlen oder Rechner zu manipulieren, wird ein Backdoor-Steuerprogramm eingeschleust, ohne dass der Anwender es merkt. Über Internet oder das lokale Netzwerk kann dieses Programm über eine Backdoor-Steuersoftware (Client) von Dritten gesteuert werden.
Cron-Dämon	Dämon, der andere Programme zu vorgegebenen Zeiten startet.
Dämon	Im Hintergrund laufender Prozess zur Systemverwaltung unter UNIX. Im Schnitt laufen einige Dutzend Dämonen auf dem Rechner. Diese Prozesse werden beim Hochfahren des Rechners gestartet.
Dazuko	Dazuko ist ein Kernel-Modul, das die Dateizugriffe an den AntiVir-Guard-Dämon weiterleitet. Siehe www.dazuko.org
Dialer	Kostenverursachende Einwahlprogramme. Auf dem Rechner installiert, bauen diese Programme eine Internetverbindung über eine Premium-Rate-Nummer auf, deren Tarifgestaltung ein breites Spektrum umfassen kann (Vorwahl 0900 in Deutschland, 09x0 in Österreich und in der Schweiz und mittelfristig auch in Deutschland). Manchmal werden Dialer bewusst unauffällig eingesetzt, bisweilen in betrügerischer Absicht. Dies kann zu horrenden Telefonrechnungen führen. AntiVir erkennt Dialer.
Engine	Modul der AntiVir-Software, das die Virensuche steuert.
Heuristik	Systematisches Verfahren, das mit generellen und speziellen Regeln bestimmte Probleme zu lösen versucht. Das Auffinden einer Lösung kann damit allerdings nicht garantiert werden. AntiVir verwendet ein heuristisches Verfahren zum Auffinden von noch unbekannten Makroviren. Hierbei wird das Makro beim Auffinden von virustypischen Funktionen als "verdächtig" gemeldet.
Kernel	Innerster Teil des Betriebssystems mit elementaren Systemfunktionen (Speicherverwaltung, Prozessverwaltung).
Logdatei	Auch: Reportdatei, Protokolldatei. Datei, in die Meldungen von Programmen geschrieben werden.
Malware	Oberbegriff für Software-"Fremdkörper" jeglicher Art. Dies können Störungen wie Computerviren sein, aber auch andere Software, die vom Nutzer generell als unerwünscht betrachtet wird (siehe auch Unerwünschte Programme).
Quarantäneverzeichnis	Verzeichnis, in das betroffene Dateien geschoben werden, um sie dem Zugriff der Benutzer zu entziehen.
root	Benutzer mit uneingeschränkten Rechten für die Systemverwaltung (entsprechend dem Administrator bei Windows).

Begriff	Erklärung
SAVAPI	Secure AntiVirus Application Programming Interface
Signatur	Kombinationen von Bytefolgen, an denen ein Virus oder ein unerwünschtes Programm erkannt werden kann.
Skript	Textdatei mit Befehlen, die von UNIX ausgeführt werden. (Entspricht etwa einer Batchdatei bei DOS).
SMP (Symmetric Multi Processing)	Linux SMP: Linux-Version für Rechner mit Parallelprozessoren.
SMTP	Simple Mail Transfer Protocol: Verfahren, auf dessen Basis Emails im Internet transportiert werden.
syslog-Dämon	Dämon, der die Meldungen diverser Programme protokolliert. Die Meldungen werden in unterschiedliche Logdateien geschrieben. Die Konfiguration des *syslog*-Dämons wird in */etc/syslog.conf* festgelegt.
Testversion	Ohne Lizenzdatei läuft AntiVir Server ausschließlich als Testversion. In der Testversion wird nur der Testvirus EICAR gemeldet. Der Zugriff auf die betroffene Dateien wird nicht blockiert. Die Update-Funktion ist eingeschränkt.
Unerwünschte Programme	Oberbegriff für Programme, die keinen direkten Schaden auf dem Rechner verursachen oder ohne Absicht des Anwenders oder Administrators installiert wurden. Hierzu zählen Backdoor-Steuerprogramme, Dialer, Witzprogramme und auch Spiele. AntiVir erkennt verschiedene Arten unerwünschter Programme.
VDF (Virus Definition File)	Virendefinitionsdatei: Datei mit den Signaturen der bekannten Viren. Diese Datei wird bei einem Guard oder Scanner Update autmotisch aktualisiert.
VFS	Virtual File System

9.2 Weitere Informationsquellen

Weitere Informationen zu verschiedenen Viren, Würmern, Makroviren und weiteren unerwünschten Programmen sind erhältlich unter http://www.avira.de/de/threats/index.html

9.3 Goldene Regeln zur Virenvorsorge

- Erstellen Sie Notfalldisketten/Startdisketten für Ihre Windows-Version sowie Ihren Netzwerkserver und die einzelnen Workstations. Notfalldisketten sind auch bei anderen Betriebssystemen hilfreich.
- Nehmen Sie Disketten nach Beenden Ihrer Arbeit immer aus dem Laufwerk heraus. Auch Disketten ohne ausführbare Programme enthalten Programmcode im Bootsektor und können Träger eines Bootsektorvirus sein.
- Fertigen Sie regelmäßig vollständige Backups Ihrer Daten an.
- Begrenzen Sie den Programmaustausch: Das gilt besonders für Netzwerk, Mailboxen, Internet und gute Bekannte.
- Prüfen Sie neue Programme vor und nach einer Installation. Liegt das Programm auf einem Datenträger komprimiert vor, lässt sich ein Virus in der Regel erst nach dem Auspacken bei der Installation finden.

Haben andere Personen einen Zugang zu Ihrem Rechner, sollten Sie folgende Spielregeln zum Schutz vor Viren beachten:

- Stellen Sie einen Computer als Testrechner zur Eingangskontrolle neuer Software, Demoversionen oder evtl. virenverdächtiger Datenträger (Disketten, CD-R, CD-RW, Wechseldatenträger) und von Downloads bereit. Trennen Sie diesen Rechner aber vom Netzwerk!
- Benennen Sie einen Datenschutzbeauftragten, der bei einer Virusinfektion für die Behandlung verantwortlich ist, und bestimmen Sie im Voraus alle zu einer Beseitigung eines Virus notwendigen Schritte.
- Organisieren Sie vorsorglich einen durchführbaren Notfallplan: Dieser kann die Schäden durch mutwillige Zerstörung, Raub, Ausfall oder Zerstörungen/ Veränderungen aufgrund von Inkompatibilitäten vermindern helfen. Programme und Massenspeicher lassen sich ersetzen; Daten, die für ein wirtschaftliches Überleben notwendig sind, nicht.
- Stellen Sie vorsorglich einen durchführbaren Schutz- und Wiederaufbauplan für Ihre Daten auf.
- Sorgen Sie für ein ordentlich installiertes Netzwerk, bei dem die Rechtevergabe vorbeugend eingesetzt wird. Es ist ein guter Schutz gegen Viren.





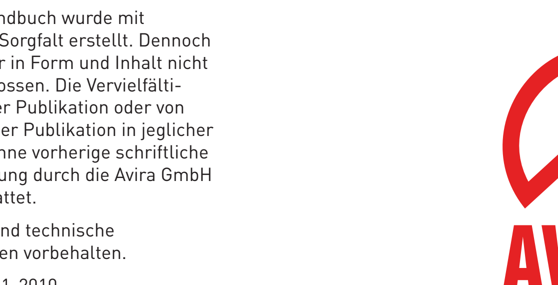
Avira AntiVir Professional | Unix

www.avira.de

Avira GmbH

Lindauer Str. 21
88069 Tettnang
Germany
Telefon: +49 (0) 7542-500 0
Telefax: +49 (0) 7542-525 10
Internet: http://www.avira.de

Ausgabe Q1-2010



AVIRA®